

(19)日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11)特許出願公表番号

特表2003-527645

(P2003-527645A)

(43)公表日 平成15年9月16日(2003.9.16)

(51)Int.Cl.⁷

G 06 F 12/00

識別記号

5 4 5

F I

テーコート(参考)

5 3 7

G 06 F 12/00

5 4 5 M 5 B 0 1 7

1/00

5 3 7 H 5 B 0 7 5

12/14

3 2 0

12/14

3 2 0 B 5 B 0 7 6

17/30

1 1 0

17/30

1 1 0 F 5 B 0 8 2

1 2 0 B

審査請求 未請求 予備審査請求 有 (全 97 頁) 最終頁に続く

(21)出願番号	特願2000-583224(P2000-583224)
(86) (22)出願日	平成11年11月15日(1999.11.15)
(85)翻訳文提出日	平成13年5月16日(2001.5.16)
(86)国際出願番号	PCT/US99/27113
(87)国際公開番号	WO00/030323
(87)国際公開日	平成12年5月25日(2000.5.25)
(31)優先権主張番号	60/108,602
(32)優先日	平成10年11月16日(1998.11.16)
(33)優先権主張国	米国(US)
(31)優先権主張番号	09/310,294
(32)優先日	平成11年5月12日(1999.5.12)
(33)優先権主張国	米国(US)

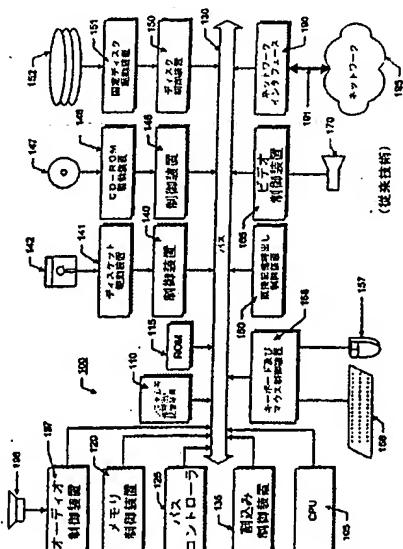
(71)出願人	イントゥー ネットワークス インク アメリカ合衆国 マサチューセッツ州 02140 ケンブリッジ ケンブリッジ パーク ドライブ 150
(72)発明者	シュマイドラー ヨナー アメリカ合衆国 マサチューセッツ州 02139 ケンブリッジ ハーバード ストリート 295
(72)発明者	アトキンス デレック アメリカ合衆国 マサチューセッツ州 02144 サマービル ファーガット アベニュー 6
(74)代理人	弁理士 金久保 勉

最終頁に続く

(54)【発明の名称】 広帯域アクセスネットワークを介してコンテンツを安全に引き渡すための方法及び装置

(57)【要約】

広帯域アクセスネットワークを介して、オンデマンドによってコンテンツを安全に引き渡すための方法は、クライアントプロセスで、承認なしにコンテンツを入手及び実行されないようにするために、1組のサーバと複数の安全機能を利用する。複数の暗号化されたタイトルが、このネットワークに接続されたコンテンツサーバに格納されている。同様にネットワークに接続されたアクセスサーバには、ネットワークアドレスと、上述のタイトルを暗号解説して実行するのに必要な種々のキーイング及び承認データが含まれている。ユーザのローカルコンピュータシステムで走るクライアントアプリケーションは、コンテンツサーバからタイトルを検索し且つユーザのローカルコンピュータシステムでタイトルを実行可能にする前に、アクセスサーバからアドレス、キーイング及び承認データを検索する必要がある。



【特許請求の範囲】

【請求項1】 ネットワークを介してコンテンツを引き渡すための方法であつて、

(a) 前記ネットワークに機能的に接続されたコンテンツサーバ上に少なくとも一つのタイトルを、実行不可能な形式で記憶する段階と、

(b) 前記ネットワークに機能的に接続されたアクセスサーバに、前記タイトルの位置識別子と前記タイトルを実行可能な形式に処理するのに必要なデータとを記憶する段階と、

(c) 前記コンテンツサーバから前記タイトルの少なくとも一部を検索する以前に、前記アクセスサーバから前記タイトルの前記位置識別子を入手することを、前記ネットワークに機能的に接続されたクライアントプロセスに要求する段階と、

(d) 前記タイトルの前記一部を実行可能な形式に処理するのに必要な前記データを、前記アクセスサーバから入手するよう、クライアントプロセスに要求する段階と、を包含する方法。

【請求項2】 (e) 前記クライアントプロセスに、前記アクセスサーバの署名を入手すると共に、前記コンテンツサーバから前記タイトルの少なくとも一部を検索する前に前記コンテンツサーバにその署名を提示するよう要求する段階を更に包含する、請求項1に記載の方法。

【請求項3】 (e) 前記クライアントプロセスが前記コンテンツサーバから前記タイトル前記タイトルの少なくとも一部を検索可能な時間を定義する時間データを、前記アクセスサーバから入手するよう前記クライアントプロセスに要求する段階を更に包含する、請求項1に記載の方法。

【請求項4】 (f) 前記の時間が満期になった時点で且つ前記コンテンツサーバから前記タイトル前記タイトルの少なくとも一部を検索する前に、新しい時間データを前記アクセスサーバから入手するよう前記クライアントプロセスに要求する段階を更に包含する、請求項3に記載の方法。

【請求項5】 ネットワークを介してコンテンツを安全に引き渡すための装置であつて、

- (a) 前記ネットワークに機能的に接続されると共に、少なくとも一つのタイトルを、実行不可能な形式で記憶してあるコンテンツサーバと、
- (b) 前記ネットワークに機能的に接続されるアクセスサーバであって、前記タイトルの位置識別子と前記タイトルを実行可能な形式に処理するのに必要なデータとを記憶するアクセスサーバと、
- (c) 前記ネットワークに機能的に接続されるクライアントシステムであって、前記タイトルの前記位置識別子と前記タイトルの前記一部を実行可能な形式に処理するのに必要な前記データとを、前記アクセスサーバから入手するように構成されたプログラムロジックを含んだクライアントシステムと、を包含する装置

【請求項6】 前記クライアントシステムが、
前記タイトルの一部を実行するよう構成されたプログラムロジックを更に包含する、請求項5に記載の装置。

【請求項7】 前記アクセスサーバが、
前記タイトルの少なくとも一部を前記コンテンツサーバから検索可能な時間を定義する時間データを生成するよう構成されたプログラムロジックを更に包含する、請求項5に記載の装置。

【請求項8】 前記クライアントシステムが、
前記の時間が満期になった時点で、新しい時間データを前記アクセスサーバから要求するよう構成されたプログラムロジックを更に包含する、請求項7に記載の装置。

【請求項9】 前記ネットワークが広帯域アクセスネットワークを包含する、
請求項5に記載の装置。

【請求項10】 ネットワークを介してコンテンツを引き渡すための装置であつて、

(A) 前記ネットワークに接続可能なコンテンツ・サーバシステムで、
(A. 1) 時間間隔を特定するデータを含くむと共にクライアントプロセスから受け取ったトークンに応答する認証プログラムロジックであつて、前記クライアントプロセスが特定の時間にメモリにアクセスする許可を受けているか

どうかを判断するよう構成された認証プログラムロジックと、

(A. 2) 前記クライアントプロセスから受け取られる共に前記メモリに記憶されたタイトルの一つを固有に特定するデータを含んだ前記トークンに応答するアクセスプログラムロジックであって、前記メモリ及び前記トークンにより固有に特定された前記タイトルに対するアクセスを可能とするよう構成されたアクセスプログラムロジックとを包含した、コンテンツサーバシステムと、

(B) 前記ネットワークに接続可能なアクセスサーバシステムであって、

(B. 1) クライアントプロセスが提供したタイトルの固有識別子に応答する変換プログラムロジックであって、前記タイトルの前記固有識別子を、前記ネットワーク上の、前記タイトルにアクセス可能なアドレスを示す位置識別子に変換するよう構成されている変換プログラムロジックと、

(B. 2) クライアントプロセスからの要求に応答するアクティベータ生成プログラムロジックであって、前記要求に応答してアクティベータを生成するアクティベータ生成プログラムロジックと、を包含するアクセスサーバシステムと、

(C) 前記コンテンツサーバ及び前記アクセスサーバシステムに前記ネットワークを介して接続可能なクライアントシステムであって、

(C. 1) 前記アクセスサーバシステムから、トークンと、アクティベータと、特定されたタイトルにアクセスできる前記コンテンツサーバの位置識別子とを入手するよう構成されたプログラムロジックと、

(C. 2) 前記コンテンツサーバから前記特定されたタイトルの少なくとも一部を検索するよう構成されたプログラムロジックと、

(C. 3) 前記コンテンツサーバから検索された前記特定されたタイトルの前記一部を実行するよう構成されたプログラムロジックと、を包含するクライアントシステムと、

を包含する装置。

【請求項11】 前記クライアントシステムが、そのシステム上で実行可能なオペレーティングシステムを更に包含し、更に、前記クライアントプロセスが、

(C. 4) 前記特定されたタイトルに関連したネットワーク・ファイ

ルシステムをマウントすると共に、前記クライアントシステムのメモリに前記タイトルに関連した複数レジストリエントリを記憶するよう構成されたプログラムロジックと、

(C. 5) タイトル実行中に前記オペレーティングシステムからの複数の要求を傍受すると共に、前記レジストリエントリに前記傍受した要求の選択部分を転送するよう構成されたプログラムロジックとを更に包含する、請求項10に記載の装置。

【請求項12】 前記アクティベータが暗号データを包含する、請求項10に記載の装置。

【請求項13】 前記アクティベータが少なくとも一つのバイトコードを包含し、更に、前記クライアントシステムが、

(C. 4) 前記アクティベータ内に含まれた前記バイトコードを解釈し且つ実行するプログラムロジックを包含する、請求項10に記載の装置。

【請求項14】 ローカルコンピュータシステム上のアプリケーションを、そのアプリケーションが前記ローカルコンピュータシステムにインストールされないなくても実行する方法であって、

(a) ネットワークマウント可能なファイルシステムと前記アプリケーションに関連した一組のレジストリエントリとにアクセスする段階と、

(b) 前記ネットワークファイルシステムをマウントする段階と、

(c) 前記レジストリエントリを前記ローカルコンピュータシステムに記憶する段階と、

(d) 遠隔源から前記アプリケーションの少なくとも一部を検索する段階と、

(e) 前記ローカルコンピュータシステムのオペレーティングシステムの制御下で前記アプリケーションを実行する段階と、

(f) 前記オペレーティングシステムからの要求を傍受する段階と、

(g) 前記傍受した要求の選択部分を、前記ローカルコンピュータシステムに記憶されたレジストリエントリに転送する段階とを包含した、アプリケーションの実行方法。

【請求項15】 プロセッサと、メモリと、1つかそれ以上のアプリケーショ

ンを実行する能力を備えたオペレーティングシステムとを備えたコンピュータシステムにおいて、アプリケーションを前記コンピュータシステムにインストールしなくとも実行するためのシステムであって、

ネットワークファイルシステムをマウントすると共に前記アプリケーションに関連した複数のレジストリエントリをメモリに記憶するように構成されたプログラムロジックと、

遠隔源から前記アプリケーションの少なくとも一部を検索するように構成されたプログラムロジックと、

前記オペレーティングシステムからの要求に応答するプログラムロジックであって、前記オペレーティングシステムからの要求を傍受すると共に前記傍受した要求の選択部分を前記レジストリエントリに転送するよう構成されたプログラムロジックとを包含する、アプリケーションを実行するためのシステム。

【請求項16】 アクセスサーバと1つ又はそれ以上のタイトルデータソースにコンピュータネットワークを介して機能的に接続されたローカルコンピュータシステム上で実行されるクライアントプロセスにおいて、タイトルのオンデマンド引き渡しを可能とする方法であって、

(a) 前記アクセスサーバからトークンと、アクティベータと、特定されたタイトルがアクセス可能なソースのネットワークアドレスとを入手する段階と、

(b) 前記トークンを前記ソースに送信する段階であって、このトークンデータが、前記ソースにアクセス可能な時間間隔を定義する、送信段階と、

(c) 前記ソースから前記タイトルの少なくとも一部を検索する段階と、

(d) 前記ソースから検索したタイトルの前記一部を実行する段階と、

(e) 前記アクセスサーバから更新されたトークンを入手する段階とを包含する、方法。

【請求項17】 前記タイトルがネットワークマウント可能なファイルシステムと、一組のレジストリエントリとを包含し、更に、前記ステップ(d)が、

d 1. 前記ネットワークファイルシステムをマウントすると共に前記レジストリエントリ記憶する段階と、

d 2. 前記ローカルコンピュータシステムで実行されているオペレーティング

システムからの要求を傍受すると共に前記傍受された要求の選択部分を前記レジストリエントリに転送する段階とを包含した、請求項9に記載の方法。

【請求項18】 プロセッサと、メモリと、ネットワークインターフェースとを備えると共に、コンピュータネットワークに接続可能なサーバ装置において、要求プロセスによるタイトルへのアクセスを可能にする方法であって、

- (a) 要求プロセスからのランチストリングを認証する段階と、
- (b) 要求プロセスから受け取ったタイトルの固有識別子を、このタイトルにアクセス可能な前記コンピュータネットワーク上のアドレスを示す位置識別子に変換する段階と、
- (c) アクティベータを生成する段階と、
- (d) 前記アクティベータを前記コンピュータネットワークを介して前記要求プロセスに送る段階とを包含する、方法。

【請求項19】 ロセッサと、メモリと、ネットワークインターフェースとを備えると共に、コンピュータネットワーク 1つかそれ以上のクライアントプロセスに接続可能なサーバ装置で用いる方法であって、

- (a) クライアントプロセスから、一定時間を特定するデータとタイトルを固有に特定するデータとを含んだトークンを前記ネットワークインターフェースを介して受け取る段階と、
- (b) 前記クライアントプロセスが特定の時間に前記タイトルにアクセスする許可を受けているかどうか判断する段階と、
- (c) 前記段階(d)において前記クライアントが許可されていれば、前記メモリと前記トークンにより固有に特定されているタイトルにアクセスする段階と
- (d) 前記トークンにより特定されている前記タイトルの少なくとも一部を前記クライアントに供給する段階とを含んだ、方法。

【請求項20】 1つかそれ以上の要求者プロセスへのタイトルのコンピュータネットワークを介した選択的引き渡しを可能とするする方法であって、

- (a) 要求者プロセスに、前記コンピュータネットワーク上のアドレスに実行不可能な形式で記憶されているタイトルの選択した部分へのアクセスを所定の条

件で提供し、

(b) 前記要求者プロセスに、前記タイトルを実行不可能な形式からの実行可能な形式への処理に有用なデータを提供する段階と、

(c) 前記タイトルが前記コンピュータ上にインストールされるのを防止する一方で、前記コンピュータシステムにおける前記タイトルの選択した部分の実行を許容する段階とを包含した、方法。

【請求項21】 タイトルをコンピュータネットワークを介して1つかそれ以上の要求者プロセスに引き渡す方法であつて、

(a) 要求者プロセスから、タイトルを特定するデータを受け取り、

(b) 前記要求者プロセスに、前記タイトルにアクセス可能な前記コンピュータネットワーク上の位置を特定するデータと前記タイトルにアクセスするのに必要な許可データとを提供する段階と、

(c) 前記要求者プロセスから支払い情報を受け取る段階とを包含した、方法

【発明の詳細な説明】

【0001】

関連出願

本願は、名称が「広帯域アクセスネットワークを介してコンテンツを安全に引き渡すための方法及び装置」であり、ヨナー・シュマイドラー等により、1998年9月16日に出願された米国仮特許出願第60/108602号に基づいて優先権を主張する。

【0002】

更に、本願は、同一発明者であるヨナー・シュマイドラー等により出願された、3件の共同所有された米国特許出願に基づいて優先権を主張する。上記出願には、

【0003】

名称が「広帯域アクセスネットワークを介してコンテンツを安全に引き渡すための方法及び装置」であり、ヨナー・シュマイドラー等により1999年5月12日に出願された米国出願第09/310294号、弁護士整理番号第A0028/7000と、

【0004】

名称が「コンテンツの安全な引き渡しシステムに於けるインストール抄録のための方法及び装置」であり、ヨナー・シュマイドラー等により1999年5月12日に出願された米国出願第09/311923号、弁護士整理番号第A0028/7001と、

【0005】

名称が「コンテンツの安全な引き渡しに於けるコンテンツ保護のための方法及び装置」という、ヨナー・シュマイドラー等により1999年5月12日に出願された米国出願第09/310299号、弁護士整理番号第A0028/7002と、

【0006】

名称が「広帯域アクセスネットワーク上でのオンデマンド配信のための方法及び装置」であり、ヨナー・シュマイドラー等により1999年5月12日に出願

された米国出願第XX/XXXXXXX号、弁護士整理番号第A0028/700
3とを包含する。

【0007】

上記で特定した同時特許出願中の発明対象は、ここで参照することにより本明細書に編入される。

【0008】

発明の分野

本発明は、一般的には、ネットワークを介してデータを分配するための方法及びシステムに関し、更に詳細には、実行可能なソフトウェアのコンテンツを、オン・デイマンド加入又は申込み（原語：subscription）が可能な様で、広帯域アクセスネットワークを介して引き渡しするためのシステムに関する。

【0009】

発明の背景

ソフトウェアアプリケーション及びオーディオ、ビデオ、アニメーション等のようなマルチメディアデータ型のオンデマンド引き渡しは、主にネットワークを介する送信速度のせいで、最近まで実用的ではなかった。一連のビットにフォーマットされるデータの送信速度は、bpsと呼ばれる。初期のモデムの情報伝達能力は、1秒当たり約300ビットの送信速度であったが、その後モデムのデータ送受信速度が増大した。このようなモデム速度の増大につれて、ネットワークを介して送信されるデータの型ばかりでなくネットワークの接続形態の性質も進歩を始めた。9600bps及び1200bpsのモデム速度では、インターネットのようなコンピュータネットワークは、主に特定のプロトコルとテキストメッセージを有するアスキーテキスト環境であった。モデム速度が引き続き増大することで、より複合的な情報がインターネット及び他のコンピュータネットワークを介してアクセスできるようになった。今日依然として、アスキーテキストバラダイムが、インターネットのワールドワイドウェブ部分に残っているが、ごく最近の帯域幅環境の増大によって、更に複合的なコンテンツ及びマルチメディアデータ型の通信が可能になってきた。

【0010】

最近では、100万bpsを超える接続速度を有する高性能広帯域技術及びケーブルモ뎀が、ケーブル通信、電話通信、移動電話通信及び衛星通信企業によって世界中で展開且つ提供されつつある。現在の広帯域アクセスネットワークには、ケーブル通信産業の媒体共有型の複合ファイバー同軸ケーブル（HFC）ネットワーク及び電話通信産業のデジタル加入者回線（xDSL）が含まれる。

【0011】

広帯域技術及び広帯域アクセスネットワークの登場によって、以前には、コンパクトディスク読み出し専用記憶素子（CD-ROM）及びデジタル多目的ディスク（DVD）でしか入手できなかった、複合的なマルチメディアデータ型及びソフトウェアタイトル（以後「タイトル」と呼ぶ）に、現在では、広帯域アクセスネットワークサービスの加入者が、遠隔地からアクセスすることができる。

【0012】

しかし、データ送信速度以外にもタイトルのオンデマンド引き渡しの実用化を阻んできた要因がある。ソフトウェア及びマルチメディアタイトルを含むコンテンツのオンデマンド引き渡しを今まで阻んできたそのような障害の1つは、タイトルを実行する上で、加入者のローカルコンピュータシステムにタイトルをロードさせるという必要性であった。更に、広範に行われているコンテンツの複製又は「海賊版製作」、及び全機能を備えたタイトルの複製の配信に伴う安全性に関わるリスクのために、オンデマンド配信は、ソフトウェア出版業者及びコンテンツライブラリにとって魅力的ではなかった。

【0013】

よって、加入者のローカルコンピュータのシステムにインストールする必要のない、実行可能なソフトウェアコンテンツを、オンデマンドで引き渡すための方法及びシステムに対する必要性が存在する。

【0014】

更に、コンテンツの価値を保護するセキュリティを提供し、且つその無断使用及び複製を防止するコンテンツを、加入者のローカルコンピュータのシステムに、オンデマンド引き渡しするための方法及びシステムに対する必要性が存在する。

【0015】

更に、コンテンツ実行中の待ち時間要件を満足させる方法で、広帯域アクセスネットワークを介してコンテンツを引き渡すことができる方法及びシステムに対する必要性が存在する。

【0016】

発明の概要

本発明の安全なコンテンツ引き渡しプラットホーム（SCDP）は、高帯域幅実行可能コンテンツを、オンデマンドで且つ広帯域アクセスネットワークを介して引き渡しを行う。このSCDPプラットホームを使用して、例えば、ケーブルモデム及びxDSLサービスの加入者のような広帯域加入者は、広帯域ネットワークを介してタイトルにアクセスできる。

【0017】

ユーザは、例えば、入手可能なタイトルの仮想カタログを表示するワールドワイドウェブ上で、仮想店舗ショーウィンドウから実行すべきタイトルを選択する。交渉には、第三者電子コマースシステム（Eコマース）にユーザ登録すること、タイトルを選択すると、ユーザはそのタイトルを実際に購入するために交渉する。ユーザ課金情報を提供すること及び選択タイトルに付随して提示される購入タイプの中から1つを選択することが含まれる。考えられる購入タイプの例としては、1) 特定のタイトルの期限付き試用、2) 任意のタイトルの「一回使用」毎の1回の支払い、3) 週極め、月極め等の一定の具体的な期間に亘るタイトルの無制限の「複数使用回」を許可する1回の支払いがある。

【0018】

購入交渉が完了すると、ユーザのパーソナルコンピュータで実行中のSCDPクライアントソフトウェアが、条件付きアクセスサーバ（CAS）から、許可トークン及びキーイングデータを入手する。このトークンによって、クライアントプロセスは、広帯域ネットワークを介してアクセス可能なネットワークファイルサーバから選択したタイトルの実行を許可される。ファイルサーバから検索されたデータは暗号化される。SCDPクライアントプロセスには、ファイルサーバからのデータを暗号解読するために、条件付きアクセスサーバによって提供され

るキーイングデータを使用する。本発明では、タイトルはユーザのパーソナルコンピュータで走るが、タイトルはそれの全体が、このパーソナルコンピュータにダウンロードされるわけではない。タイトルは電子的なパッケージの中にフォーマットされており、そのパッケージには、圧縮且つ暗号化された形式で、タイトルのファイルが含まれている（以後 b r i q と呼ぶ）。この b r i q は、実際には、ポータブルな、独立言語ファイルシステムであり、特定のタイトルを実行するのに必要なファイルが全て含まれている。b r i q は、広帯域ネットワークを介してアクセス可能なネットワークファイルサーバ（以後 R A F T サーバと呼ぶ）に格納されている。SCDPクライアントは、b r i q を、ユーザのパーソナルコンピュータのローカルファイルシステムの如く取扱う。タイトルを実行する場合、例えばウインドウズ（R）のようなオペレーティングシステムが、このようなローカルファイルシステムに読み出しを要求する。図示された実施例では、ウインドウズ（R）仮想デバイスドライバ（V x D）を含むSCDPクライアントが、RAFTサーバから、b r i q データの要求されたブロックを検索することによって、このような要求に応える。データの要求されたブロックを検索後、V x D が、b r i q データを圧縮且つ暗号化し、そのデータを、ユーザのパーソナルコンピュータのオペレーティングシステムに送る。

【0019】

本発明の1つの態様によれば、ソフトウェアタイトルが、ターゲットコンピュータに「インストール」されることは決してない。SCDPクライアントソフトウェアによって、1つのインストール抽象が創り出され、現在実行中のタイトルはホストコンピュータにインストールされている、という錯覚を、オペレーティングシステムに対して維持する。従って、タイトルの実行が終了すると、システム上にはタイトルが実行されたという形跡は何も残らない。タイトルに関連するファイルは、パーソナルコンピュータのハードディスクには何も残らず、更にタイトルに関連するレジストリ変数などのオペレーティングシステムの状態情報も一切残存しない。タイトルの利用者は、ゲームなどで獲得した「レベル」のような、プレイ全般に亘って維持することが望ましいと思われる、ある種の状態情報を保存するオプションを有する。このような状態情報は、後述のライトスループ

ファイルに保存できる。

【0020】

本発明の別の態様によれば、SCDPクライアントソフトウェアは、本発明の所有権を主張できるランダムアクセスファイル転送(RAFT)プロトコルを使用して、広帯域ネットワークを介して b r i q データを検索する。このプロトコルは、SCDPクライアントに、RAFTサーバに格納されているファイル及びディレクトリへの読み出し専用アクセスを提供する。b r i q は1つのローカルファイルシステムとして取り扱われる所以、RAFTクライアントは、1つのオペレーティングシステムドライブとして存在が認識される必要が無く、又オペレーティングシステムのファイルシステムマネージャ、即ち図示された実施例におけるウインドウズ(R)・インストラブル・ファイルシステム(IFS)マネージャに、インターフェースをとる必要がない。従って、RAFTクライアントファイルシステムドライバ、即ち図示された実施例におけるVxDは、遠隔又はネットワークファイルシステムドライバよりも小さく、単純である。更に、RAFTプロトコルは、「帯域幅スロットリング」のようなダイナミック帯域幅の制限をサポートし、又RAFT許可トークンの使用を通じてアクセス制御をサポートする。

【0021】

本発明の別の態様によれば、SCDPは、種々の安全機能を用いて、無断アクセス及びリプレイからコンテンツを保護する。許可トークン及び暗号解読キーは、条件付きアクセスサーバから入手する。SCDPクライアントとCAS間のネットワーク通信は、安全な遠隔手続き呼び出し(RPC)インターフェースを介して保護される。一旦、安全チャネルがSCDPとCAS間で確立されると、SCDPクライアントは、選択されたタイトルのRAFT許可トークン及びキーイングデータを要求する。この許可トークンは、CASからの符号化されたメッセージであり、それによって、要求を行っているユーザが、特定の b r i q に、特定のRAFTファイルサーバで、また交渉済みの支払タイプで明確にされた期間、アクセスできることを表す。

【0022】

RAFT許可トークンによって、SCDPクライアントがタイトルの b r i q へのアクセスを許されても、このSCDPクライアントは、タイトルのファイルデータへアクセスするのに b r i q を、例えば、圧縮解除及び暗号解読など更にアンパックしなければならない。CASによって、ユーザは b r i q データを暗号解読するのに必要なキーイングデータを提供されるが、CASは、SCDPクライアントにキーイングデータを直接提供するわけではない。直接提供する代わりに、CASは、暗号解読アルゴリズムを実行する曖昧化したバイトコードにキーを埋めることによって、キーイングデータをユーザから隠す。孤立したキーイングデータをSCDPクライアントに引き渡すのではなく、CASは、曖昧化したバイトコード（以後アクティベータと呼ぶ）を引き渡す。SCDPクライアントの仮想デバイスドライバが、バイトコード解釈プログラムでこのアクティベータを実行することで、b r i q データの暗号解読を行う。コード曖昧化によって、アクティベータを逆行分析するのが困難になり、ハッカーは、このアクティベータからキーイングデータを取り出すためには、かなりの時間と資源を費やさねばならぬ、一般的には、そのコストは保護されているコンテンツの価値以上になる。本発明の意図するところでは、アクティベータは、1件のクライアント当たり、1つの b r i q 当たり、また1回の実行当たり只1つであり、即ち、CASから入手されるアクティベータは、それぞれ異なっており、且つ只1回だけ使用可能である。そうすることで、複数回使用するユーザーに対して、1回ごとの、コストの掛かる逆行分析を行なおうとする気持ちにさせない。

【0023】

本発明によれば、RAFT認証トークン及びアクティベータには、共に限られた寿命が設定されている。認証トークンには満了期間が含まれており、それ以後は無効となる。実行中のアクティベータは、一定の時点で、自己更新のためにCASと交換を開始する。その交換に失敗すると、アクティベータが動作不能になり、従ってタイトルは動作不能になる。アクティベータの更新を、以後、アクティベータ保持と呼ぶ。この保持機能の結果、現在実行中のアクティベータに、新たなキー、データ又はコードすらも含みうる最新版が引き渡されることになる。認証トークンが更新されるとアクティベータも更新される。新たな認証トークン

は、暗号解読用キーイングデータと一緒に、この新たなアクティベータ内に埋込まれる。始動時に、更新アクティベータが、SCDPクライアント内のRAFT・VxDへ新たなRAFT認証トークンを引き渡す。

【0024】

SCDPシステムは媒体非依存であり、ユーザとネットワークサーバ間に、現在実行中のCDタイトルの時間要件を満足させるのに十分な帯域幅が存在していれば、HFCネットワーク及び電話企業のデジタル加入者回線を含む、任意の広帯域ネットワーク技術全般で動作するものである。またSCDPシステムは、10メガbps及び100メガbpsのイーサネット(R)・ローカルエリアネットワークを使用しても実現でき、例えば、同じようにインターネットを介して実行可能なコンテンツを引き渡すための企業ネットワーク内でも実行できる。

【0025】

本発明の第1の実施例によれば、ネットワークを介してコンテンツを引き渡すための方法が、(a)前記ネットワークに機能的に接続されたコンテンツサーバ上に少なくとも一つのタイトルを、実行不可能な形式で記憶する段階と、(b)前記ネットワークに機能的に接続されたアクセスサーバに、前記タイトルの位置識別子と前記タイトルを実行可能な形式に処理するのに必要なデータとを記憶する段階と、(c)前記コンテンツサーバから前記タイトルの少なくとも一部を検索する以前に、前記アクセスサーバから前記タイトルの前記位置識別子を入手することを、前記ネットワークに機能的に接続されたクライアントプロセスに要求する段階と、(d)前記タイトルの前記一部を実行可能な形式に処理するのに必要な前記データを、前記アクセスサーバから入手するように、クライアントプロセスに要求する段階と、を包含する。

【0026】

本発明の第2の実施例によれば、ネットワークを介してコンテンツを安全に引き渡すための装置が、(a)前記ネットワークに機能的に接続されると共に、少なくとも一つのタイトルを、実行不可能な形式で記憶してあるコンテンツサーバと、(b)前記ネットワークに機能的に接続されるアクセスサーバであって、前記タイトルの位置識別子と前記タイトルを実行可能な形式に処理するのに必要な

データとを記憶するアクセスサーバと、(c) 前記ネットワークに機能的に接続されるクライアントシステムであって、前記タイトルの前記位置識別子と前記タイトルの前記一部を実行可能な形式に処理するのに必要な前記データとを、前記アクセスサーバから入手するように構成されたプログラムロジックを含んだクライアントシステムと、を包含する。

【0027】

本発明の第3の実施例によれば、ネットワークを介してコンテンツを引き渡すための装置が、(A) 前記ネットワークに接続可能なコンテンツ・サーバシステムであって、(A. 1) 時間間隔を特定するデータを含むと共にクライアントプロセスから受け取ったトークンに応答する認証ロジックであって、前記クライアントプロセスが特定の時間にメモリにアクセスする許可を受けているかどうかを判断する認証ロジックと、(A. 2) 前記クライアントプロセスから受け取られる共に前記メモリに記憶されたタイトルの一つを固有に特定するデータを含んだ前記トークンに応答するアクセスプログラムロジックであって、前記メモリ及び前記トークンにより固有に特定された前記タイトルに対するアクセスを可能とするアクセスプログラムロジックとを包含した、コンテンツサーバシステムと、(B) 前記ネットワークに接続可能なアクセスサーバシステムであって、(B. 1) クライアントプロセスが提供したタイトルの固有識別子に応答する変換プログラムロジックであって、前記タイトルの前記固有識別子を、前記ネットワーク上の、前記タイトルにアクセス可能なアドレスを示す位置識別子に変換するよう構成されている変換プログラムロジックと、(B. 2) クライアントプロセスからの要求に応答するアクティベータ生成ロジックであって、前記要求に応答してアクティベータを生成するアクティベータ生成ロジックと、を包含するアクセスサーバシステムと、(C) 前記ネットワークに接続可能なクライアントシステムであって、(C. 1) 前記アクセスサーバシステムから、トークンと、アクティベータと、特定されたタイトルにアクセスできる前記コンテンツサーバの位置識別子とを入手するよう構成されたプログラムロジックと、(C. 2) 前記コンテンツサーバから前記特定されたタイトルの少なくとも一部を検索するよう構成されたプログラムロジックと、(C. 3) 前記コンテンツサーバから検索された前

記タイトルの前記一部を実行するよう構成されたプログラムロジックと、を包含するクライアントシステムと、を包含する。

【0028】

本発明の第4の実施例によれば、ローカルコンピュータシステム上のアプリケーションを、そのアプリケーションが前記ローカルコンピュータシステムにインストールされていなくても実行する方法が、(a) ネットワークマウント可能なファイルシステムと前記アプリケーションに関連した一組のレジストリエントリとにアクセスする段階と、(b) 前記ネットワークファイルシステムをマウントする段階と、(c) 前記レジストリエントリを前記ローカルコンピュータシステムに記憶する段階と、(d) 遠隔源から前記アプリケーションの少なくとも一部を検索する段階と、(e) 前記ローカルコンピュータシステムのオペレーティングシステムの制御下で前記アプリケーションを実行する段階と、(f) 前記オペレーティングシステムからの要求を傍受する段階と、(g) 前記傍受した要求の選択部分を、前記ローカルコンピュータシステムに記憶されたレジストリエントリに転送する段階とを包含する。

【0029】

本発明の第5の実施例によれば、アプリケーションをコンピュータシステムにインストールしなくても実行するためのシステムが、ネットワークファイルシステムをマウントすると共に前記アプリケーションに関連した複数のレジストリエントリをメモリに記憶するように構成されたプログラムロジックと、遠隔源から前記アプリケーションの少なくとも一部を検索するように構成されたプログラムロジックと、前記オペレーティングシステムからの要求に応答するプログラムロジックであって、前記オペレーティングシステムからの要求を傍受すると共に前記傍受した要求の選択部分を前記レジストリエントリに転送するよう構成されたプログラムロジックとを包含する。

【0030】

本発明の第6の実施例によれば、タイトルのオンデマンド引き渡しを可能とする方法が、(a) 前記アクセスサーバからトークンと、アクティベータと、特定されたタイトルがアクセス可能なソースのネットワークアドレスと入手する段

階と、(b) 前記トークンを前記ソースに送信する段階であって、このトークンデータが、前記ソースにアクセス可能な時間間隔を定義する、送信段階と、(c) 前記ソースから前記タイトルの少なくとも一部を検索する段階と、(d) 前記ソースから検索したタイトルの前記一部を実行する段階と、(e) 前記アクセスサーバから更新されたトークンを入手する段階とを包含する。

【0031】

本発明の第7の実施例によれば、要求プロセスによるタイトルへのアクセスを可能にする方法が、(a) 要求プロセスからのランチストリングを認証する段階と、(b) 要求プロセスから受け取ったタイトルの固有識別子を、このタイトルにアクセス可能な前記コンピュータネットワーク上のアドレスを示す位置識別子に変換する段階と、(c) アクティベータを生成する段階と、(d) 前記アクティベータを前記コンピュータネットワークを介して前記要求プロセスに送る段階とを包含する。

【0032】

本発明の第8の実施例によれば、ロセッサと、メモリと、ネットワークインターフェースとを備えると共に、コンピュータネットワーク 1つかそれ以上のクライアントプロセスに接続可能なサーバ装置で用いる方法が、(a) クライアントプロセスから、一定時間を特定するデータとタイトルを固有に特定するデータとを含んだトークンを前記ネットワークインターフェースを介して受け取る段階と、(b) 前記クライアントプロセスが特定の時間に前記タイトルにアクセスする許可を受けているかどうか判断する段階と、(c) 前記段階(d)において前記クライアントが許可されていれば、前記メモリと前記トークンにより固有に特定されているタイトルにアクセスする段階と、(d) 前記トークンにより特定されている前記タイトルの少なくとも一部を前記クライアントに供給する段階とを含んでいる。

【0033】

本発明の第9の実施例によれば、1つかそれ以上の要求者プロセスへのタイトルのコンピュータネットワークを介した選択的引き渡しを可能とするする方法が、(a) 要求者プロセスに、前記コンピュータネットワーク上のアドレスに実行

不可能な形式で記憶されているタイトルの選択した部分へのアクセスを所定の条件で提供し、(b) 前記要求者プロセスに、前記タイトルを実行不可能な形式からの実行可能な形式への処理に有用なデータを提供する段階と、(c) 前記タイトルが前記コンピュータ上にインストールされるのを防止する一方で、前記コンピュータシステムにおける前記タイトルの選択した部分の実行を許容する段階とを包含する。

【0034】

本発明の第10番目の実施例によれば、タイトルをコンピュータネットワークを介して1つかそれ以上の要求者プロセスに引き渡す方法が、(a) 要求者プロセスから、タイトルを特定するデータを受け取り、(b) 前記要求者プロセスに、前記タイトルにアクセス可能な前記コンピュータネットワーク上の位置を特定するデータと前記タイトルにアクセスするのに必要な許可データとを提供する段階と、(c) 前記要求者プロセスから支払い情報を受け取る段階とを包含する。

【0035】

本発明の第11番目の実施例によれば、コンピュータネットワークを介して1つかそれ以上の要求者プロセスへ機能的に接続されたコンピュータシステムで使用されるコンピュータプログラム製品が、

(a) 前記ネットワークに接続された要求者プロセスから選択したタイトルを特定するデータを検索するよう構成されたプログラムコードと、(b) 前記要求者プロセスから支払い情報を受け取るよう構成されたプログラムコードと、(c) 前記要求者プロセスが、前記タイトルの選択した部分にアクセスしてダウンロードするのを可能にするよう構成されたプログラムコードと、(d) 前記タイトルがコンピュータシステム上での実行は許容する一方、前記タイトルの前記コンピュータシステムへのインストールは防止するよう構成されたプログラムコードと、を包含する。

【0036】

実施例の詳細な説明

図1に示すのは、カリフォルニア州パロアルトのサン・マイクロシステムズ社から市販されているサンスパークステーション5ワークステーション又はニュー

ヨーク州アーモックのインターナショナル・ビジネス・マシーンズ社から共に市販されているIBM RS/6000ワークステーション又はIBMアプティバ・パーソナルコンピュータのようなコンピュータシステム100用のシステムアーキテクチャであり、このようなアーキテクチャ上で本発明を実施することができる。図1のコンピュータシステムは、説明目的の例示にすぎない。この説明で、特定のコンピュータシステムを説明する際に共通して使われる用語に言及する場合があるが、本説明及び概念は、図1と異なるアーキテクチャを有するシステムを含め、他のシステムにも等しく該当する。

【0037】

コンピュータシステム100は、従来のマイクロプロセッサを用いて実行可能な中央演算処理装置(CPU)105、情報の一時記憶用のランダムアクセスメモリ(RAM)110及び情報の永久記憶用の読み出し専用記憶素子(ROM)115を包含する。メモリ制御装置120は、RAM110を制御するために配設されている。

【0038】

バス130は、コンピュータシステム100の構成要素を相互接続する。バスコントローラ125は、バス130を制御するために配設されている。割込み制御装置135は、システム構成要素からの種々の割込み信号を受信及び処理するために用いられる。

【0039】

大容量記憶装置は、ディスクケット142、CD-ROM147又はハードドライブ152であってもよい。データ及びソフトウェアは、ディスクケット142及びCD-ROM147のような取外し可能な媒体を介して、コンピュータシステム100とやり取り可能である。ディスクケット142は、ディスクケット駆動装置141へ挿入可能であり、その駆動装置は制御装置140を介して、更にバス30に接続している。同様に、CD-ROM147は、CD-ROM駆動装置146へ挿入可能であり、その駆動装置は制御装置145を介して、更にバス130に接続している。ハードディスク152は、制御装置150を介してバス130に接続されている固定ディスク駆動装置151の一部をなす。

【0040】

コンピュータ100へのユーザ入力には、複数の装置がなりうる。例えば、キーボード156及びマウス157が、制御装置155を介してバス130に接続されている。マイクロホンとしても又スピーカとしても動作可能なオーディオトランジューサ196が、図に示すように、オーディオ制御装置197を介してバス130に接続されている。ペン及び／又はタブロイドのような他の入力装置が、必要であればバス130及び適切な制御装置やソフトウェアに接続されることは、通常の技能を備えた当業者には明らかであろう。DMA制御装置が、RAMに対して直接記憶呼出しを実行するために配設されている。視覚的表示は、ビデオ表示装置170を制御するビデオ制御装置165によって生成される。コンピュータシステム100には、バス191及びネットワーク195によって概略的に示されているように、このコンピュータシステムがローカルエリアネットワーク（LAN）又は広域ネットワーク（WAN）と相互接続するを可能にする通信アダプタ190も包含されている。

【0041】

コンピュータシステム100の動作は、ワシントン州レドモンドのマイクロソフト社から市販されているウインドウズ（R）95又はウインドウズ（R）NTのようなオペレーティングシステムソフトウェアによって全体的に制御及び調整される。このオペレーティングシステムは、システム資源の割付けを制御し更に、とりわけ、処理スケジュール、記憶域管理、ネットワーキング及び出入力サービスのようなタスクを実行する。特に、システム記憶装置に常駐し、CPU105で走るオペレーティングシステムは、コンピュータシステム100のその他の構成要素の動作を調整する。本発明は、OS/2（登録商標）、UNIX（R）、Linux及びSolaris（登録商標）を含む任意の数の市販されているオペレーティングシステムを用いて実行してもよい。ネットスケープ・コミュニケーションズ社から市販のネットスケープナビゲーターのバージョン2.0以上及びワシントン州レドモンドのマイクロソフト社から市販のインターネットエクスプローラのバージョン1.0以上等の1つ又はそれ以上のブラウザアプリケーションが、これらのオペレーションシステムの制御下で実行できる。

【0042】

SCDPシステムの概説

図2Aに概念的に図示されているのは、本発明による安全なコンテンツ引き渡しプラットホーム（SCDP）システム200及び広帯域ネットワーク環境におけるその他の要素であり、このような環境は例示目的のためにすぎず限定を意図したものではない。図2Aに示す要素によって、本発明が簡便化され且つ理解されるはずである。図2Aで示されたり、又はここに説明されている要素は、本発明の実施又は動作にとって必ずしも全てが必要であるわけではない。図2Aに示す如く、SCDPシステム200は、条件付きアクセスサーバ（CAS）210、付随のCASデータベース212、ランダムアクセスファイル転送サーバ（RAFT）206、RAFTデータベース208及びSCDPクライアント216を包含する。

【0043】

CASサーバ210、RAFTサーバ206及びSCDPクライアント216に加えて、本発明は、仮想店舗ショーウィンドウ215及びEコマースサーバ202の使用を意図している。Eコマースサーバ202は、付随する課金データベース204を有する。店舗ショーウィンドウ215は、付随するデータベース213を有する。例示の実施例では、サーバ202、210及び215が、ローカルイーサネット（R）ネットワークのような、専用の、安全なローカルエリアネットワーク（LAN）を介して接続されている。そのLANは更に、インターネットサービスプロバイダ（ISP）230を介して、図2Aのインターネットクラウド240として示されているように、広域コンピュータネットワークトポロジに接続されている。MC I・WorldCom、AT&T、アメリカオンライン等の任意の商業利用可能なインターネットアクセスサービスプロバイダを、ISP230として使用してもよい。例示の実施例では、サーバ202、210及び215が、専用ローカルエリアネットワークを介して接続されているものとして示してあるが、このようなサーバは、インターネットのような他の非専用ネットワークを介して機能的に接続されてもよいことは、当業者には明らかであろう。更に、Eコマースサーバ202が、金融又は銀行機関（図示せず）のクレジッ

ト取扱いサーバに接続されることで、クレジットカード及び／又は別種の取引の取扱いを促進する。

【0044】

再び図2Aを参照すると、図1と同様のアーキテクチャを有する、1つ又はそれ以上のクライアントパーソナルコンピュータが、広帯域アクセスネットワーク203及びケーブルプロバイダ207を介してSCDPシステム200に接続されている。例示の実施例では、ケーブルモデム(CM)は、SCDPクライアントが実行しているホストコンピュータに接続する。次いで、複数のケーブルモデムが、高周波接続を経由してケーブルノードに連結されている。一般的には、1000ものホストパーソナルコンピュータが、適切なケーブルモデム及び高周波接続を介して1つのケーブルノードに接続しうる。各ケーブルノードは、更にケーブルモデム終端システム(CMTS)を介して終端ヘッドエンドに接続されている。複数のケーブルモデムが、1つの終端ヘッドエンドに接続されている。複数の相互接続されたヘッドエンドは、広帯域アクセスネットワークの中核を構成する。これらのケーブルヘッドエンドは、ケーブル会社の施設に配置されているのが一般的であり、更にT1回線又は別の接続を介して、インターネットプロトコル(IP)ネットワークに接続されているホストデータ端末装置を含んでもよい。このT1回線は、更にインターネットサービスプロバイダ(ISP)230を介してインターネットに接続されうる。RAFTサーバ206及びそれに付随するデータベース208が、インターネットサービスプロバイダ230と、ケーブル会社が提供するホストデータ終端施設又はヘッドエンドとの間で、広帯域アクセスネットワーク203に接続されている。このようにして、RAFTサーバ206は、SCDPシステム200の一部をなすが、CAS210、Eコマースサーバ202及び仮想店舗ショーウィンドウ215から遠隔配置されている。ケーブルモデム終端システム209は、ケーブル通信施設からの高周波データを、公開されているケーブル経由データサービス工業規格(DOCSIS)を適用して、インターネットプロトコルフォーマットに変換する。

【0045】

或いは、図2Aで示すように、クライアント・パーソナルコンピュータを、デ

ジタル加入者回線（D S L）経由で、S C D Pシステム2 0 0に接続してもよい。このような構成では、S C D Pクライアントが実行されているホストコンピュータは、D S Lモデム及び既存の一般の交換電話回線施設を経由して電話会社のスイッチと接続される。

【0 0 4 6】

D S L加入者ネットワーク及び広帯域アクセスネットワークの構造は、本発明の分野では公知であり且つケーブル会社及び電話会社によって現在広範に使用されているので、簡略のために此处ではこれ以上詳しく説明することは控えたい。よって、必ずしも上記説明のシステムの全要素が図2 Aで示されているわけではない。

【0 0 4 7】

加入手順

図2 Bは、S C D Pシステム2 0 0内の構成要素の相互作用を概念的に示したものである。図4 A乃至4 Bのフローチャートは図2 Bの概念ブロック図と合わせて、加入処理及びランチ（原語：launch）処理中にS C D Pシステム2 0 0が実行する本発明による処理ステップを示す。

【0 0 4 8】

パーソナルコンピュータ上でネットスケープ・ナビゲータ又はマイクロソフト・インターネットエクスプローラのようなH T M Lブラウザを実行中のS C D Pクライアント2 1 6を使用しているユーザは、ステップ4 0 1に示したように仮想店舗ショーウィンドウ2 1 5からタイトルを選択する。店舗ショーウィンドウ2 1 5では、入手可能な各タイトルは、汎用資源ロケータ（U R L）内部に埋め込まれたデジタルオッファーとして表示してある。このデジタルオッファーは選択したタイトル及び購入タイプを特定する情報を含んでいる。ステップ4 0 2に示したように、デジタルオッファーを選択すると、加入者のブラウザをEコマースサーバ2 0 2のH T T Pフロントエンド2 0 2 Aに送る。ステップ4 0 3に示したように、ユーザは、デジタルオッファーU R L内の情報に基づきEコマースサーバ2 0 2と購入交渉する。この交渉にはユーザ登録とクレジット情報の提供が通常含まれる。

【0049】

ステップ404Aに示したように、Eコマースサーバは、購入を特定し且つ許可する情報を含んだランチストリングを生成する。この情報には所望のコンテンツを固有に特定する汎用資源名(URN)が含まれる。このURN及びランチストリングの形式及び記述は後に説明する。ステップ404Bに示したように、ランチストリングは、CAS210によってデジタル署名され、SCDPクライアント216に送達するためにEコマースサーバ202に送信される。

【0050】

ランチストリングは、MIME(多目的インターネットメッセージ拡張仕様)ヘッダでパックされている。ステップ405に示したように、ランチストリングがSCDPクライアントのブラウザ224に受け取られると、ランチストリングに関連付けられたMIMEタイプをレジストリエントリ内に探し出し、その結果としてSCDPクライアント216内部のランチャモジュール220が呼び出されることになる。ステップ406Aに示したように、ランチャ220はCAS210と安全な接続を確立して、CASが指定したURNのURLを提供するようつまりURNからURLへの変換を要求する。URLは該当するbriqデータの位置を特定する。CAS210は該当するURLをランチャ220に送る。ステップ406Bに示したように、一旦ランチャは対応するbriqデータの位置を特定すると、ランチストリングを含んだ購入要求をCASに送る。

【0051】

ステップ407に示したように、CASはランチストリングの署名を確認して、RAFT許可トークン及びアクティベータをランチャに返す。アクティベータ及び許可トークンは後に詳しく説明する。許可トークンはアクティベータ内部に埋め込まれていてもよい。次に、ステップ408に示したように、ランチャはアクティベータをARFSD・VxD218に渡すことでタイトルをランチする。ARFSD・VxDはアクティベータを実行し、RAFT許可トークンをRAFT・VxD222に回す。ステップ409に示したようにRAFT・VxDはURLを開けてヘッダを読む。RAFT・VxD222は、ステップ410に示したように最初の許可トークンをRAFTサーバに送る。ステップ411に示した

ように、RAFT・VxD 222はRAFTサーバ206からのコンテンツを読み始め、受け取ったコンテンツをARFSD・VxD 218に戻す。ステップ412に示したように、ARFSD・VxDは、アクティベータを用いてbrinqデータ形式のコンテンツを解読及び復元解凍し、更に、解読データのブロックに保全性チェックを行う。

【0052】

その後、ステップ413に示したように、オペレーティングシステムはARFSD・VxDが提供するローカルファイルシステムを介してタイトルを実行する。アクティベータはランチャ220に対し定期的に要求して、CAS210にアクティベータ及びRAFT許可トークンを更新させる。ステップ414に示したように、最初の要求が出されると、CASは購入をEコマースサーバ202に通知して、取引が成立つまり完了する。最初のアクティベータの寿命は数分程度の場合もある。第1回目のタイムアウト後に正しくアクティベータが更新されると、このタイトルがうまく実行されていることを示す。

【0053】

システム構成要素及びそれらの相互作用の大筋をこうして説明したところで、本発明の安全なコンテンツ引渡しシステム200及びそこで実行される処理を図3A乃至14を参照して説明する。

【0054】

SCDPクライアント

図3Aを参照すると、本発明によるSCDPクライアント216の概念ブロック図を示す。SCDPクライアント216により、ユーザはホスト・パーソナルコンピュータ上でbrinq符号化されたタイトルを実行できる。図3Aに示したように、SCDPクライアントは、ランチャ220、アレバ・ファイルシステム・ドライバVxD (ARFSD・VxD) 218、及びRAFTクライアントVxD 222を包含する。SCDPクライアント216は、オペレーティングシステム219（例えば、本実施例ではウィンドウズ(R) アプリケーション）上を実行可能なアプリケーションとして実現してもよい。図1を参照して説明したように、オペレーティングシステム219はIBM・PC又はその他のコンピュー

タ・アーキテクチャのようなパーソナルコンピュータ・アーキテクチャ上で実行可能である。SCDPクライアント216に加え、ブラウザ217（一般的にはネットスケープナビゲーター又はマイクロソフト・エクスプローラなどのHTMLブラウザ）は、オペレーティングシステム219の制御下に実行してもよい。ランチャ220、ARFSD・VxD218及びRAFT・VxD222は、後に図3B乃至3Dをそれぞれ参照してより詳しく説明する。

【0055】

図3Bは、SCDPクライアント216のランチャ220を包含するプログラムロジックモジュールのブロック図を概念的に示す。具体的には、ランチャ220は、制御モジュール300、CAS・RPCライブラリ302、ARFSD・VxD通信ライブラリ304、及びユーザインターフェース306を包含する。図示した実施例では、ランチャ220はSCDPクライアントとCAS204との間の全ての通信を調整するロジックを含んだウインドウズ(R)・アプリケーションとして実現してもよい。Eコマースシステム202との購入交渉が完了すると、ランチャ220はクライアントのウェブブラウザ217に呼び出される。Eコマースシステムは、クライアント・ウェブサーバにランチャに関連したIMEタイプ付きのランチストリングを送る。更に、ランチャはCASとの全ての通信を管理するが、その通信には1) CASからのRAFTサーバのアドレス及び選択したタイトルに対応するbriqパス名を入手、2) RAIDサーバからbriqデータを検索し、検索したデータを解読するのに必要なRAFT許可トークン及びアクティベータのCASからの入手、及び3) RAID許可トークン及びアクティベータをCASに対して更新依頼することが含まれる。

【0056】

CASサーバ206とARFSD・VxDモジュール218との間の通信を容易にするため、ランチャ220は、CAS・PRCライブラリ302を含む。このライブラリは遠隔手続き呼出し(RPC)ライブラリを介してCASサーバ206との間で通信を行う一連のオブジェクト又はプログラムコードとして実現できる。モジュール302に適したRPCライブラリとしては、ノーブルネット社から市販されているノーブルネット安全RPCプロダクトがある。オプションで

、ネットスケープ・コミュニケーションズ社が発行した安全ソケットライブラリ（SSL）規格に準拠したネットワーク移送製品を用いて、RPC呼び出しをネットワーク上で移送して、本発明のシステム内のSCDPクライアントとの通信安全性を向上させてもよい。通信ライブラリを、ランチャ・モジュール220とARFSD・VxDモジュール218との間の通信と、ARFSD・VxDモジュール218とRAFTクライアントVxD222との間の通信に用いてもよい。こうしたライブラリは、ランチャ220とVxD218とのデータ通信に必要なコード又はオブジェクトを含んでいてもよい。例えば、後に詳しく説明するように、`briq1200`の`briq`ヘッダ1202は、図12に示すように、タイトルを実行中に制御モジュール300によって読まれ、通信ライブラリ304を介してVxD218に提供される。

【0057】

ランチャ220を呼び出すと、グラフィック・ユーザインターフェース(GUI)がユーザインターフェース306を介してユーザに表示される。図示した実施例では、ユーザインターフェース306は、ウィンドウを作成し、そうしたウィンドウ内でグラフィック情報を表示し、キーボード、マウス、その他の位置決め装置を介してユーザからコマンドを受けるためにウィンドウズ(R)・オペレーティングシステムに含まれたオペレーティングシステム・インターフェース及びアプリケーションプログラム・インターフェース(API)とのインターフェースをとるため適切なプログラムロジック及び/又はオブジェクトを含む。また、こうしたユーザインターフェースは通常の技能を備えた当業者の理解範囲に十分はあるものである。このGUIを介して、ユーザはディスク・キャッシュサイズなどのユーザの好む設定を行うことができ、エラー状態も通知される。

【0058】

制御モジュール300は、タイトルをランチすると共にSCDPクライアント200とCAS210とRAFTサーバ206との間の通信を継続するのに必要なアルゴリズムを実行するのに適したコード又はオブジェクトで実現できる。更に具体的には、制御モジュール300が実行するアルゴリズムは図4A乃至6及び関連した本明細書箇所により詳細に説明してある。

【0059】

図3Cは、図3BのARFSD・VxD304の概念的ブロック図である。VxD304は、バイトコード・インターフリタ308、制御モジュール304、及びARFSD・VxD通信ライブラリ312を包含する。ARFSD・VxD304は仮想デバイスドライバであり、オペレーティングシステムがbrinqデータをローカルファイルシステムとして読めるようにする。ARFSD・VxD304はbrinqデータを解凍解除及び解読する。更に、ARFSD・VxDは、例えばウインドウズ(R)・レジストリエントリを提供するなどインストール抄録(言語:abstract)を保持する。ARFSD・VxDはオペレーティングシステムのアクセス呼び出しを全て傍受し且つ実行中だがディスクに保存はされないタイトルに関連したレジストリエントリをシミュレートして、動的レジストリエントリを実現する。

【0060】

アクティベータ及びバイトコード・インターフリタ

上述したように、アクティベータ228は、ARFSD・VxD304内部に実現したバイトコード・インターフリタ308上で実行する。アクティベータはCAS210から入手し、ARFSD・VxD304によるbrinqデータ解読に用いるSCDPクライアントソフトウェアの一部である。アクティベータの形式と内容は図13を参照にして詳しく説明する。アクティベータは、CAS210に替わりとなる新しいアクティベータを定期的に要求するようアクティベータに求める保持機能を実現する。よって、タイトル実行を継続するには、CASとの通信は維持しなければならない。図示した実施例では、アクティベータ228内の保持機構は数値ストリングとして、又は図13を参照にして説明したように実現してもよい。

【0061】

アクティベータは、ARFSD・VxD304内で実行できる動的バイトコードオブジェクトとして実現される。図7のアクティベータ・ファクトリモジュール710を参照して既に説明したように、CASは、外部ライブラリ内に常駐させててもよいアクティベータ生成ルーチンを呼び出してアクティベータを生成する

。 R A F T トークンは上述したようにアクティベータと共にパッケージしてある。アクティベータはいずれタイムアウトし、その後は S C D P クライアント 216 は C A S を呼び出し、新しいアクティベータを要求しなければならない。アクティベータの寿命はアクティベータのトークン部分に含まれた開始及び終了時間値により決定される。

【0062】

S C D P システム 200 は、アクティベータを用いて S C D P クライアント 216 へ渡された暗号データを保護する。アクティベータは、 A R F S D ・ V x D 304 内で走ると共に b r i q の解読を可能にする一片の曖昧化バイトコードとして実現できる。アクティベータがダウンロードされると、更なる R P C を C A S 210 に対して行い、キーイングデータの送信を完了してもよい。アクティベータ内でのコード曖昧化によりキーの抽出を防ぐことができる。

【0063】

アクティベータの図示した実現例は、アクティベータ内のキーを守るために遠隔実行を用いる。遠隔実行によりアクティベータは不完全になる。つまり、遠隔実行はアクティベータが連続動作するのに十分な情報を与えるが、アクティベータが新たにコード又はデータを要求する必要がある。 A R F S D ・ V x D 304 内のバイトコード・インターフリタ 308 は、アクティベータから暗号キーデータを抽出するプログラムロジック、コード、又はオブジェクトを包含する。図示した実施例では、アクティベータは図 13 を参照して説明したような形式及び内容を備えていればよい。

【0064】

別の実施例では、アクティベータが曖昧化バイトコードを含むより高度なアクティベータの実現例を用いるが、 A R F S D ・ V x D 304 内のバイトコード・インターフリタ 308 はリッチ命令セットを用いて実現し、曖昧化を単純にできる機会を増やしてもよい。ハードウェアが実現するマイクロプロセッサ命令セットにあった従来の制限が無く、アドレス指定方式及び命令形式用に多くのビットを用いることができる。こうした命令セットの複雑さ及び機密性により、 S C D P システム内のコンテンツ引き渡しの安全性を確保する。バイトコードは V x D

内で走るため、バイトコード・インタープリタ308は、他のVxDからエクスポートされたインターフェースを呼び出すかもしれないが、オペレーティングシステムからのWIN32機能を呼び出す必要もなく、DLLを扱う必要もない。

【0065】

図示した実施例においては、バイトコード・インターパリタ308は、CAS210から受け取ったアクティベータ内のバイトコードを解釈及び実行するのに必要な適切なコード及び／又はプログラムロジックを備えた仮想計算機として実現してある。こうした仮想計算機は、バイトコードを翻訳し、バイトコードストリームからの一時データを全て保存し、バイトコードにより特定される処理を実行するための適切な経路を備えている。バイトコード・インターパリタ308を如何に具体的に実現するかは、従って、インターパリタにより実行可能なバイトコードセットに依存する。例えば、バイトコード・インターパリタ308は、アクティベータが含むコードの種類に対応するために幾つかの次に挙げたものを含んだ特定の機能を実行可能である。

- ・ビット式オペレータ — 暗号化及び配列化ルーチンに有用なけた送り、回転、及び「ビット抽出」機能。
- ・評価 — バイトコード・インターパリタにダウンロードした又は変更したバイトコードを解釈させ、よってコード及びデータが対応するフラグ及びデータ保護から分離されるのを防ぐ。
- ・インターフェース基本命令（言語：primitive） — SCDPクライアント
- ・バイトコード・インターパリタが、引数配列化およびCタイプの特定の事前定義データセットの内部化を含む、他のVxD内の機能を直接呼び出す。SCDPクライアント及びCASは安全ストリームインターフェース基本命令を用いる。例えば、接続データ（特に認証データ）をアクティベータ又は手法が生成されたストリームから抽出するフック。

【0066】

通常の技能を備えた当業者であれば、バイトコード・インターパリタ308は物理的計算機として実現してもよいことは明らかであろう。本明細書に記載した最も単純なアクティベータにおいては、バイトコードはオプションである。よつ

て、バイトコード・インターフリタ308もオプションとしてもよい。

【0067】

通信ライブラリ312は、ARFSD・VxDモジュール218とRAFT・VxDモジュール222との間の通信用に用いられる。こうしたライブラリは図3Bの通信ライブラリ304に類似したもので、VxD218とVxD220との通信を助ける。

【0068】

制御モジュール310には、インストール抄録を実行し、タイトルを実行し、且つRAFTトークンを更新するのに必要なアルゴリズムを実行するのに必要なプログラムロジック又はコードが含まれる。更に詳細には、制御モジュール310が実行するアルゴリズムは、図4A乃至6及びそれに関する記載箇所に更に詳しく説明してある。

【0069】

図3Dは、SCDPクライアント216のRAFTクライアントVxD222を包含する構成要素の概念ブロック図を示す。詳しくは、VxD222は、RAFT・RPCライブラリ316、キャッシングロジック318、及び制御モジュール320を包含する。RPCライブラリ316は、本明細書に更に詳しく説明しているが、RAFTプロトコルのクライアント側RPCレイヤを実現する適切なコード及び/又はオブジェクトを含む。こうしたプログラムロジックは、RAFTメッセージの何れかを用いるRAFTサーバ206との通信に使用される。具体的には、モジュール316は、図11を参照して説明するように、RAFTパケットヘッダを各RAFTプロトコルメッセージに添えるため、且つ適切なRAFTプロトコルメッセージで応答するために必要なロジックを含む。キャッシングロジック318は、RAFTプロトコルを用いてRAFTサーバ206から検索したbriq、又はその一部のキャッシングを行うための適切なコードを含んでいる。モジュール218によりキャッシングされたbriqの部分は、SCDPクライアント216が実行しているホストパーソナルコンピュータの一時メモリの一部に保存してもよい。具体的なキャッシング技法及びそれに関連したロジックは、多数ある周知のキャッシングアルゴリズムに従って実現でき、それは通常の技能を

持った当業者に容易に理解可能である。制御モジュール320は、モジュール316、318に関する上述の機能を管理し且つ図4A乃至6に関連して記載した方法の諸ステップを実行するために必要なプログラムロジック、コード及び／又はオブジェクトを含むように実現される。

【0070】

タイトル実行

図5A乃至5Cのフローチャートは、本発明による典型的なタイトル実行中にSCDPクライアント216により実行される処理ステップを示す。上述したように、SCDPクライアントのブラウザ224がランチストリングを受け取ると、ランチストリングに関連した多目的インターネットメッセージ拡張仕様(MIME)タイプがレジストリエントリで探し出され、その結果、SCDPクライアント216内のランチャモジュール220が呼び出される。ステップ6に示したように、呼び出しに起こると、ランチャ220はランチストリングから汎用資源名(URN)を抽出して、CAS210にURNからURLへの変換を要求する。本発明のURNはbrig:内的のタイトルの固有識別子である。標準URN形式は以下の通りである。

urn:arepa://vendor/path/titlename[#version]

【0071】

URNにおいては、タイトルへのパスは、ベンダの記憶サーバ内にあるタイトルの現在の位置に正確に一致している必要はない。このパスは分類の便宜を図るものであり、必要ではない。タイトルのバージョン番号はオプションであり、pond記号でタイトル名から分離してもよい。ベンダ名は固有性を保証するために中央権威機関に登録してもよい。

【0072】

汎用資源ロケータ(URL)は、RAFT記憶サーバ内にあるbrig:内的の現在の位置を特定する。標準URL形式は以下の通りである。

raft://hostname/path/brigname.brig

【0073】

URLにおいては、パスはRAFT記憶サーバ内にあるbrig:内的の現在の位置

に正確に一致していなければならない。

【0074】

図5A乃至5Cは、本発明による加入及びタイトル実行中にSCDPクライアント及び内部モジュールにより実行される処理ステップを示す。図2Bの要素も参照すると、SCDPクライアントが走るホストコンピュータのユーザは、ウェブブラウザ224を用いて、仮想店舗ショーウィンドウ215から所望のタイトルを選択する。店舗ショーウィンドウ215はデジタルオッファをウェブブラウザに返すが、ユーザはこのオッファを用いてEコマースサーバ202と購入交渉を行う。Eコマースサーバは、未署名のランチストリングをネットワークを介してウェブブラウザに送信する。ランチストリングはMIMEヘッダでパックされている。ステップ502に示したように、ランチストリングがブラウザに受信されると、ランチストリングに付随したMIMEタイプは、ファイルシステムのレジストリエントリで探し出され、その結果、SCDPクライアントのランチャモジュール220が呼び出されることになる。処理ステップ504に示したように、ランチャモジュール220はランチストリングからURN値を抽出して、このURN値をCASサーバ210に送信する。ランチャ220とCAS210との通信は安全なRPC接続を介して確立される。CAS210はURNをURLに変換し、当該URLをSCDPクライアントに送信する。URLが受け取られるとき、決定ステップ506に示したように、ランチャ220はURLヘッダを読み出す要求をARFSD・VxDモジュール218に渡し、モジュール218はその要求をRAFTクライアントVxD222へ、そしてARFSD・VxDモジュール218及びランチャ220に戻される。この処理全体は図5Aの処理ステップ508に示されている。次に、処理ステップ510に示したように、ランチャモジュール220は、ヘッダの内容を用いてホストシステムのアプリケーション検査要求を実行する。

【0075】

システムの検査要求の完了後に、処理ステップ512に示したように、ランチャモジュール220は購入許可要求を、安全なRPC接続を介してCAS210に送信する。購入許可要求に応答して、CAS210はRAFTトーカンを含んだアクティベータを生成すると、アクティベータは安全なRPC接続を介してSCDPクライアント216に送信される。決定ステップ514に示したようにアクティベータを受け取ると、ステップ516に示したように、ランチャモジュール220はRAFTトーカン及びアクティベータをインストールする。処理ステップ516及び518にそれぞれ示したように、アクティベータはARFSD・VxDモジュール218内にインストールされ、VxDモジュール218は、RAFTトーカンをRAFTVxD内にロードする。処理ステップ520に示したように、RAFT・VxD222は、その後、RAFTプロトコルからの適切な命令の何れかを用いてRAFTトーカンをRAFTサーバ206に送信する。次に、処理ステップ522に示したように、ARFSD・VxD218は、VxD222との通信を介してRAFTサーバ206にあるbrinqからスーパー ブロックフィールドを読み出し、処理ステップ524に示したように、スーパー ブロック内のマジックナンバーを検査する。brinq内のマジックナンバーは、例えば「ARFS」などの固定キャラクタ列（原語：constant sequence of characters）として実現してもよい。

【0076】

この時点で、処理ステップ526に示したように、ランチャモジュール220はタイトルの実行可能ファイルを実行し始める。図示した実施例では、実行可能ファイルは、RAFTVxD222を介して入手したデータを用いてARFSD・VxD218が実現したファイルシステム中に位置したWindows(R)実行可能ファイルの形式となっている。

【0077】

処理ステップ528に示したように、RAFT・VxD222は、RAFTサーバ206からタイトルディレクトリ及びファイルの検索を開始する。タイトルのディレクトリ及びファイルを包含するデータブロックは、RAFTプロトコル及び本明細書に記載されたコマンドを用いてRAFTサーバ206から入手する

。詳しくは、VxD222は、データブロックをRAFTサーバ206から読み出し開始（言語：read-ahead）方式で入手し、データブロックをキャッシングして効率的な解読及び実行を促進する。

【0078】

処理ステップ530に示したように、ARFSD・VxD218は、CASアクティベータ210から検索したアクティベータ、特に解読キーデータを用いてRAFTサーバ206から入手したデータブロックを解読し、且つ保全性検査を行う。上述したように、アクティベータには、briq内にあるデータを実行前に解読するのに役立つ暗号か情報が含まれている。処理ステップ532に示したように、ARFSD・VxD218は、オペレーティングシステムに対してインストール抄録を保持して、タイトル実行に必要なファイルシステムがローカルホスト・パーソナルコンピュータにインストールされているかのような錯覚を作り出す。VxD218がインストール抄録を保持する処理は、図6を参照して詳しく説明する。

【0079】

CAS210から受け取ったRAFTトークンは、図8を参照して説明してあるように終了時間フィールドを含む。決定ステップ534及び処理ステップ536に示したように、アクティベータ及びRAFTトークンが満期つまり無効となる前に、ランチャモジュール220は安全なRPC接続を介して、更新アクティベータ及びRAFTトークンのペアをCASサーバ206に要求する。処理ステップ538に示したように、この新しいアクティベータ及びRAFTトークンのペアは上述した方法と同様にインストールされ、使用される。

【0080】

インストール抄録

本発明によれば、タイトルはSCDPクライアントホストシステム上に「インストール」されることはない。SCDPクライアントソフトウェアはインストール抄録を作成して、実行中のタイトルがホストコンピュータにインストールされているという錯覚をローカル・オペレーティングシステムに対して維持する。よって、タイトル実行が終了すると、タイトルがホスト・パーソナルコンピ

ュータ上で実行されたことを示す証拠は残らない。タイトルに関連した如何なるファイルもホストシステムのハードディスク上に残らず、例えばタイトルに関連したレジストリ変数などのオペレーティングシステム状態情報も残らない。タイトルが出た後又はシステムクラッシュ後のSCDPクライアントの状態は、以前と同じである。可能性は低いが唯一の例外は、例えば、他のアプリケーションが行った処理、持続性状態及び保存した文書又はデータなどのユーザがアプリケーションに対して行った変更によるものである。インストール抄録は、アプリケーションを実行する前に予想されるアプリケーションの状態をロードする方法で達成されるが、これは、アプリケーションが出る際に、持続性パラメータに影響を与えずにこの状態がアンロードされるように行われる。

【0081】

図12に関連して説明されているように、本発明による各 $b_r i q$ は1つからそれ以上のタイトルのファイルシステムを含む。以下に説明するように、 $b_r i q$ オーサーは、オーサユーティリティプログラムを用いて、アプリケーション及びアプリケーション・インストールディレクトリから選択したファイルを抽出する。 $b_r i q$ オーサーは、アプリケーションを正しく実行するのに必要かもしれないレジストリエントリのようなそれ以外の情報も抽出する。オーサープログラムは、選択したファイルと他の情報を組合せ、且つデータベースエントリセット及び $b_r i q$ 形式でファイルシステムを出力として生成する。この $b_r i q$ はRAFTサーバに記憶される。データベースエントリはCASサーバに記憶され、キーイング情報及びヘッダチェックサム値などの情報を包含する。

【0082】

図6は、本発明による、タイトル実行中にインストール抄録を保持するために、SCDPクライアント216及び内蔵されたモジュール218乃至220によって実行される処理ステップを示したフローチャートである。ステップ600に示したように、あるタイトル選択及び購入交渉に続いて、ランチャ220及びRFSD・VxD218はファイルシステムをマウントし、ステップ602に示したように、関連したレジストリエントリをホストシステムのローカルドライブに記憶する。ウインドウズ(R)95、ウインドウズ(R)98、及びウインド

ウズ（R）NTのファイルマネージャ内の機能及びUNIX（R）オペレーティングシステムの同等の機能は、ファイルディレクトリ及び遠隔位置ファイルの内容を「マウント」し、又はそれらへのコンピュータネットワークを介したアクセスを実現し、データをアクセスする「仮想ドライブ」を生成する。本発明では、ファイルシステムのマウントは、RAFTサーバにSCDPクライアント・オペレーティングシステムインターフェースを介してアクセスするための上述した技法を用いることを包含する。ファイルシステムをマウントすると、タイトルコンテンツ及びそのタイトルに関連したレジストリエントリを含むb r i qからデータブロックの全部又は一部はキャッシュすることになり得る。この一連のレジストリエントリはSCDPクライアントのホストシステムメモリにローカル記憶され、タイトルファイルがインストールされたディレクトリなどの情報を含むことができる。ARFSD・VxD218は更に、CASデータベース212から適切なデータベース項目を抽出する。

【0083】

ステップ604に示したように、CASサーバによりSCDPクライアントに送られたアクティベータからのキーイング情報を用いて、b r i qからのデータブロックは解読され、且つオペレーティングシステム・ファイルシステムとして実行される。タイトル実行中は、データブロックは必要に応じてSCDPクライアントでローカルキャッシュされる。プログラム実行中に、オペレーティングシステムの仮想メモリマネージャ部分内に含まれるようなオペレーティングシステムのデバイスドライバは、ローカル物理ドライブに記憶させたレジストリエントリを要求する。決定ステップ606に示したように、アプリケーションが実行されると、ARFSD・VxD218はこうした処理要求の解釈を開始する。ステップ608に示したように、該当する場合は、呼び出しは、局所記憶されているレジストリエントリのリストからのエントリで満足される。しかし、後に記載するライトスルー手法を用いてオペレーティングシステムに直接書き込まれる情報もある。

【0084】

決定ステップ610に示したように、アプリケーション実行が終了するまでは

、オペレーティングシステム呼び出しの傍受及び局所記憶されたレジストリエントリを用いたこれら要求の満足は継続される。この時点で、ステップ612に示したように、ランチャはARFSD・VxD218にファイルシステムをアンマウントつまり切断するよう指示する。その結果、オペレーティングシステム要求は局所記憶されたレジストリエントリに転送されなくなる。局所記憶されたレジストリエントリ及び局所でキャッシュされたデータブロックは消去されるか、上書きしてもよい。その結果、タイトルつまりアプリケーションを実行する前のSCDPクライアントの状態は、ユーザが意識的に保持しようと願う限られたライトスルーデータを除いてはそのタイトルのインストールの痕跡もなく現状に戻される。

【0085】

ライトスルーフォルダ記憶

作成者プログラムを用いたオーサーによるbriqの生成時に、ファイル及びディレクトリは「ライトスルーフォルダ」属性のタグを付けることができる。ライトスルーファイル又はディレクトリを内包するbriqは、LOC Lタグ付きのコンテナを内包していることがある。このコンテナは全てのライトスルーディレクトリの完全なパス及び、LDI Rタグで示される、ライトスルーファイルを内包するあらゆるディレクトリ（ルートディレクトリを除く）のパスを含む。ユーザは局所記憶ファイル用のルートディレクトリのパス名を指定することができる。新しいパス名は、固有性を確保するため、URNからのベンダフィールドを含む。この情報は、タイトルのLOC Lコンテナ内のROOTタグに記憶される。デフォルトでは、ARFSD・VxDは、ローカルドライブに0バイトの空きがあると報告する。ライトスルーファイル又はディレクトリを含まないbriqは常に0バイトの空きがあると報告する。タイトルのLOC Lコンテナ内にタグが存在すれば、ARFSD・VxDが、局所記憶ディレクトリを内包するドライブ上の空きスペース量を報告するはずであることを示す。タイトルがLOC Lコンテナを必要とするのは、ROOTに関してフォールト値以外を指定する必要がある場合のみである。

【0086】

ライトスルーファイル又はディレクトリを内包した b r i q (言い換えれば、ヘッダに LOCL コンテナを内包した b r i q) がロードされると、SCDP クライアント内のランチャが局所記憶用のディレクトリを SCDP インストールディレクトリの下に作成する。このディレクトリは、タイトルの LOCL コンテナ内で ROOT タグによって他のディレクトリが指定されていなければ、URN から導き出す。ランチャは、ヘッダに LDIR タグを付けて指定された各ディレクトリ用の局所記憶ディレクトリ内にサブディレクトリを作成する。局所記憶パスのルートパス名及び空きディスクスペースを報告するかどうかを b r i q ロード中に ARFSD・VxD に渡す。ランチャソフトウェアがアンインストール及びオプションでタイトルが出る時に、局所記憶領域内の全てのファイルは消去される。これらの局所記憶されたファイルはデフォルトでは持続性がある。ランチャは、b r i q 内の全てのライトスルーディレクトリ用のディレクトリをローカル記憶装置内に作成する必要がある。

【0087】

ライトスルーファイルが開始されると、情報は、上述したディレクトリと同様の命名規則を備えた局所記憶領域内のファイルから取り出される。もしそのファイルが局所記憶装置に存在しない場合は、そのファイルはまず b r i q からコピーされる。b r i q 内の元々のファイルは、全 b r i q 暗号化を別にすれば圧縮や暗号化されていないこともある。ライトスルーファイルを開くと、ローカルディスクのコピーも開かれて、ARFSD・VxD ファイルハンドルにおける全ての要求は実ファイルハンドルで実行される。

【0088】

条件付きアクセスサーバ (CAS)

図 7A は、条件付きアクセスサーバ (CAS) 700 及び付随したデータベース 750 の概念プロック図である。図示した実施例では、CAS は、POSIX_1 (IEEE 標準 1003.1, 1998 年) に互換性のあるプラットフォーム上で実行可能なアプリケーション (例えば、カリフォルニア州パロアルト所在 のサンマイクロシステムズ社が市販するサンソラリス (Sun Solaris (商標)) オペレーティングシステム又は、レッドハットソフトウェア社が市販するリナッ

クスオペレーティングシステム)として実現してもよく、こうしたプラットフォームは図1に示したものと類似のコンピュータアーキテクチャ上で実行できる。CASアプリケーション702は、データベース・インターフェースモジュール704、遠隔手順呼び出しインターフェース706、URN-URL変換モジュール708、アクティベータファクトリ710、及びURL検証モジュール712を更に包含する。

【0089】

データベースインターフェースモジュール704はCASデータベース750とのインターフェースを取り、市販のデータベース製品を用いて実現してよい。データベース750は、更新を要求するトークンのステイデータなどの短期ステイデータ又は、タイトル名、暗号キー情報及びSCDPシステムを介して入手できるタイトルに関する他の情報などの長期ステイデータを記憶するのに用いることができる。ネットワーク上に複数のCASサーバが存在していれば、データベース750は複数のCASサーバ700が共有してもよい。データベースインターフェース704及びデータベース750は、SQL標準データベース問合わせ言語で通信する。SQL標準は、米国規格協会(ANSI)が発行している。データベースインターフェース704は、サーバ700により受け取られた問合せにフィルタをかける一組のオブジェクトを包含する。こうしたフィルタは、データベース問合わせの範囲を狭めカストマイズするのに役立つ。

【0090】

CASサーバ700はネットワーグ205を介して残りのSCDPシステムに接続され、このネットワークは図示した実施例においては、ローカルエリアネットワーク又は広域ネットワークとして実現されたインターネットプロトコルに基づいたネットワークである。サーバ700は遠隔手順呼び出しモジュール706を介してネットワーク205とインターフェースをとる。モジュール706は、サンマイクロシステムズ社が発行するオープンネットワーク・コンピューティング遠隔手順呼び出し標準(インターネット工学プロジェクトチームが発行したRFC1057)に準拠したコード又はオブジェクトを包含してもよい。こうしたRPC標準は、ネットワークを介して遠隔通信を試みる2つの実体間のフロー及

び機能呼び出しを制御するコードを定義する。モジュール706は、遠隔手順呼び出しをサブルーチン機能呼び出しのように見せる何れかの市販ツールを用いて実現してよい。モジュール706を実現するのに有用な製品の一例としては、マサチューセッツ州サウスボロ所在のノープルネット社が販売するノープルネット安全RPCがある。ノープルネット安全RPCは、通常のRPCインターフェースに付加的な安全レイヤを提供する。

【0091】

URN-URL変換モジュール708は、URN問合わせをデータベース750に受けると対応するURLを返すコード又は一連のオブジェクトを包含する。こうしたURNは、SCDPクライアントのランチャモジュールからネットワーク205を介して受け取られる。URNが記憶されるデータベース750は複数レコードを備えた順次データベースでよい。モジュール708は適切な問合わせをデータベースインターフェース704に送り、データベースから適切なURLを受け取る。モジュール708は、その後、ネットワーク上をRPCモジュール706を介して対応するURLをSCDPクライアントに送信する。或いは、タイトル及び／又はコンテンツサーバの数が限られている環境においては、URLはサーバに付随したディスクに記憶してもよく、更に、モジュール708は受信したURNの参照用テーブル変換を実行するプログラムロジックを包含していてもよい。

【0092】

変換モジュール708は、抄録URNデータ構造を絶対URLデータ構造に変換し、又、一連の変換テーブル及び関連した比較ロジックによって実現してよい。URL検証モジュール712は、Eコマースサーバ202からランチストリング及び、ハッシュコードと暗号化キーによりランチストリングがデジタル署名するタイムスタンプを受信するコード又は同等のオブジェクトを包含する。具体的には、メッセージ認証コードをCASサーバ700から受け取ったランチストリングに追加してもよい。このメッセージ認証コードは、MD5ハッシュアルゴリズムに基づいて生成されたハッシュコードを含んでもよく、更にデータ暗号化規格(DES)を含む複数の暗号化標準に従って生成された暗号化キーを含んでいい

てもよい。本明細書で説明したように、デジタル署名されたランチストリングはその後、Eコマースサーバ202に送られ、更に、クライアントホストシステムのウェブブラウザに返信される。

【0093】

SCDPシステムにおいては、アクティベータは、キーイング情報を安全でない可能性のあるクライアントプロセスに送る機能を果たす。サーバ700のアクティベータ生成モジュール710は、一連のバイトコードを生成すると共に暗号キーをその一連のバイトコードに添えるコード又は適切なオブジェクトを包含する。ある実現化例ではこのキーはデータベース750から検索される。アクティベータ生成モジュールの実現様態は、SCDPシステム内で用いられるアクティベータの洗練度に部分的に左右される。一連のバイトコード及びそこに付加又は統合されたたキーを包含するアクティベータに関しては、アクティベータ生成モジュール710は上述のように実現されている。別の実施例では、キーはアクティベータにもっと安全な方法（例えば、キーをバイトコード列に折り疊む）で統合されており、付加的ロジック及び／又はオブジェクトがモジュール710内でそうした機能を実現するのに必要である。例えば、キーを一連のバイトコードに添える替わりに、数を生成したりその他の論理演算を実行するような一定の機能を実行するバイトコード列をアクティベータ内に挿入してもよい。こうした実施例では、モジュール710は、複数のバイトコード列から何れかを無作為に選択するロジック又はコード曖昧化技法として本明細書で説明した技法を含んでもよい。こうした実施例では、モジュール710は、極めて安全にアクティベータを無作為に生成する能力を備える。或いは、更に高度に洗練されたアクティベータの実現例では、アクティベータモジュール710は、外部ライブラリに常駐することもできるアクティベータ生成ルーチンを呼び出してアクティベータを生成できる。

【0094】

上述したCASモジュールは、SCDPシステム内に5つの主たる機能を含んでいる。第1に、CASは、ユーザーに暗号化briqコンテンツの一度だけの使用を許容する暗号アクティベータを提供する。第2に、CASにより、SCDP

システムがタイトルの使用を確実且つ的確に追跡し、更に不正使用する目的で設計されたハッキングされたクライアントを開発することが極めて困難な安全モデルを確実にサポートする。第3に、CASはCAS専用キーで署名し且つアクティベータに添付された制限寿命RAFT許可トークンを提供する。RAFTクライアントは、許可トークンにRAFT要求を含める。RAFTサーバはこのトークンを用いて要求されたコンテンツにアクセスする権利がクライアントにあるか検証する。第4に、CASはEコマースサーバソフトウェア・請求書作成システムと対話し、取引を完了する。取引は、購入交渉中には完了せず、エンドユーザがコンテンツを成功裏に実行したことをCASが確認するまで行われない。第1アクティベータ更新の終了が、タイトルがうまく実行されていることを示す。5番目の機能として、CASはタイトル使用報告及びアクティベータ追跡のためのデータベースを維持する。

【0095】

3種類の経過記録がCASに関係している。第1に、CASの活動は標準UNIX(R)テキスト経過記録に記録される。この経過記録は診断のためだけに意図されている。第2に、CASは、報告及びアクティベータ追跡目的で取引をCASデータベーステーブルに記録する。これらの記録は、実際の請求書作成目的で用いられるEコマースサーバシステムによる記録とは別ものである。第3に、CASデータベース自身が内部処理経過記録を保持し、その機能は確実にデータベース処理が完了し且つロールバックされるように保証することである。こうした機能はCASデータベースに内部化してもよい。図示した実施例では、CASは、オラクルソフトウェア社から市販されているような市販のデータベースメインテンナンスソフトウェアを用い、購入処理が行われたかロールバックされたかを確認する。データベース処理は、上述した金融処理とは異なる。金融処理がデータベース処理であることもあるが、ユーザ名を更新するなどのその他多くの処理がデータベース処理でありえる。

【0096】

図示した実施例では、CASは、システム管理者がCASの状態（例えば、現在使用されているデータベース接続スレッドの数及びユーザ接続の現在の数、つ

まり、使用されている接続スレッド)を監視できる管理インターフェースをサポートする。更に、ユーザ数及び運転開始以降のデータベース接続の数のピークなどの統計情報や、運転開始以降にユーザ又はデータベース接続が所定限度に達した回数も利用できる。

【0097】

SCDPクライアントはクライアントライブラリを用いてCASと対話する。クライアントライブラリは各クライアントプラットフォームに固有であってもよいが、その訳は、これはSCDPクライアントGUIと通信するプラットフォーム固有方法を用いるからである。図示した実施例では、つまりWIN3.2プラットフォームでは、クライアントライブラリはCASLIB3.2と称する。クライアントライブラリは、CASへの移送を示すCASインターフェースクラスCCASと、特定のクライアントセッションを示すCCassessionとをエクスポートする。アプリケーション・プログラム・インターフェース(API)により、CASLIB3.2クライアントは、複数セッションを通じて複数タイトルに関する交渉を同時に実行できる。APIは、CASインターフェースを移送プロトコルの細部から隔離する役目を果たす、CASとやり取りする情報を示す追加クラスもエクスポートする。こうした方法は、CActivator、CURIなどとして実現できる。CCASは、ウィンドウズ(R)メッセージを送ってクライアントにも非同期的に応答する。

【0098】

CASによるアクティベータサポート

アクティベータの最も単純な実現例は、所与のbriqのキーをアクティベータにコンパイルしたバイトコードルーチンである。このアクティベータ実現例では、CASは、クライアントを認証し、購入したbriqを特定し、アクティベータバイトコードを構築し、更に、アクティベータをダウンロードする。SCDPクライアントは、その後、接続を閉じてタイトルを実行する。こうしたアクティベータは前もって生成しておき、CASアクティベータファクトリ710及びインターフェース704によりデータベースから直接検索してもよい。

【0099】

より高度なアクティベータ実現例では、アクティベータは暗号アルゴリズムを認識し、CASからキーを要求する。CASは認証情報及び安全データを存在するストリームから受け取っており、必要などんな引数を備えた「要求キー」に対する所定のRPC応答を用意できる。

【0100】

別の実現例では、アクティベータは複数段階を必要とする可能性もある新規な機構の任意コードを備えていてもよい。後に説明するように、アクティベータは、不透明引き数を備え且つ「テクニック」の指定付きの遠隔手順呼び出しをCASに発してもよい。その後、CASは、この不透明データをこのテクニックに送り、テクニックはオペックデータをクライアントに返すか、他の呼び出し又はその他のサービスに呼び出しを行う。CAS自信がインタプリタを備えていれば、CASはアクティベータ及びテクニックのコードをデータベースから検索できる。全てのアクティベータが予め生成されれば、いずれのテクニックに関して多くのアクティベータが存在し得る。或いは、曖昧化及び多くの曖昧化具体例を如何に組み合わせるかに関する規則集のデータベースをCASに管理させてもよい。

【0101】

CASは、所与のクライアント、製品、購入品に適したアクティベータを選択する。CASは、そのアクティベータを届け、付加的RPCを介してそのアクティベータを「サポート」する。例えば所与のbrinqに対する単純な「要求キー」などの多くのCAS・RPCを予め定義できる。こうしたRPCは選択したアクティベータに基づいて制限できる。例えば、殆どのクライアントは、単純な「要求キー」呼び出しを許可されないが、アクティベータによる使用をテクニックが予期する如何なる呼び出しでも実行することが必要となる。

【0102】

図7Bを参照すると、加入及びタイトル実行処理中にCASサーバ700が実行する処理ステップが示されている。具体的には、CASサーバ700は、図9及びそれに関連した記載で説明されているように、ランチストリングを受け取るが、ステップ720に示したように、送信元はEコマースサーバである。次に、

ステップ722に示したように、CASはランチストリングに署名する。CASは、専用暗号キーでこのランチストリングに「署名」する。処理ステップ724に示したように、署名済みのランチストリングは、その後CASサーバ700から、広帯域ネットワークに接続されたホストシステムで実行されているSCDPクライアントに送られる。図5A乃至5Cに関連して説明したように、SCDPクライアントはランチストリングからURNを抽出し、このURNをCAS700に送信する。ステップ726に示したように、CAS700はこのURNをSCDPクライアントから受け取り、処理ステップ728に示したように、URNからURLへの変換を行う。上述したように、CAS700は、モジュール708を用いてこのURN-URL変換を行う。こうした変換はデータベース750へ問合せたり、テーブル参照アルゴリズムを使用することもあるが、それはモジュール708の実現方法による。処理ステップ728に示したように、CAS700は、URLリストをSCDPクライアントに送信する。次に、処理ステップ730に示したように、CAS700は、SCDPクライアントから許可要求を受け取る。SCDPクライアントからのこの購入許可要求はランチストリングを含む。その後、処理ステップ732に示したように、CAS700は、ランチストリングを検証して、このランチストリングが以前に自分が署名したものか、複数条件付きアクセスサーバを含む実現例であれば、別の権限付与されたサーバが署名したものかを判断する。本明細書で説明したように、CASサーバのモジュール710の実現方法に従ってアクティベータは生成される。

【0103】

処理ステップ736に示したように、次に、CAS700は、RAFTトークンとアクティベータをSCDPクライアントに送信する。CAS700は、データベース750からRAFTトークンを検索する。このRAFTトークンは、本明細書で説明し、図8に示した形式を備えている。本明細書で説明したように、アクティベータ及びRAFTトークンにより、SCDPクライアントは所望のタイトルにアクセスし、タイトルデータの実行を開始できる。この段階で、決定ステップ738に示したように、アクティベータトークン更新要求がSCDPクライアントから送られるまでは、このSCDPクライアントに関しては何の動作も

行わない。処理ステップ740に示したように、SCDPクライアントから最初の更新要求を受け取ると、CAS700は、タイトル購入をEコマースサーバに通知する。この取引のEコマースサーバへの通知には、ユーザがこの特定タイトルの代金を支払ったことを示す実際の応答記録が含まれる。タイトルがSCDPクライアント上で正しく実行されていることを示す第1更新要求が出されるまで、こうした通知はなされない。CASからSCDPクライアントに当初送られたアクティベータ内のタイムアウト機構は、所定の期間後に無効つまり満了となり、タイトルが適切に実行されていることを表す。CASは、処理ステップ742に示したように、新しいトークンを発行し、要求しているSCDPクライアントにこのペアを送信する。RAFTトークンの寿命は、RAFTトークンの開始時間及び停止時間フィールドに示してあるように、アクティベータと共にSCDPクライアントに最初に送信されたトークンの寿命より長くてもよい。SCDPクライアントからのその後のアクティベータ／トークン更新要求があつても、CASがEコマースサーバにタイトル購入を通知することはない。上述したように、SCDPクライアントとCASとの間の全ての通信は、安全なRPC接続を介するので、こうした接続はRPC標準に準拠する市販の製品を用いて確立させてよい。

【0104】

通常の技能を備えた当業者なら理解するだろうが、図7Dで概観した処理は、SCDPクライアントとの、タイトル実行終了と共に終わる関係においてCASが実行する諸ステップに注目したものである。CASは、幾つかの異なるスレッドが図示した処理の様々なステップを同時実行するマルチタスク・アプリケーションとして実現できることは、通常の技能を備えた当業者には明白であろう。従って、CASは特定のSCDPクライアントの要求を満たす一方、同時に他のSCDPクライアントからの要求にも対応可能である。

【0105】

RPC移送

CASとCASLIB32は、ノーブルネット安全RPCなどの標準に基づいた遠隔手順呼び出しライブラリを介して通信する。SCDPクライアントはCA

Sに複数の呼び出しを同期で行い、C A Sはこれら呼び出しを処理のためスレッドに割り当てる。C A S L I B 3 2は非同期的インターフェースを接続されたG U Iに提供し、それはこれらの同期R P C要求をキューに入れ且つ背景スレッドから取り出す。高い処理能力を提供するため、C A Sは、タスク実行のために用いることができるスレッドを準備してプールしておく。このスレッドプールは再使用可能なC ++クラスである。入ってくるタスクはR P Cレイヤで捕捉され、スレッドプールのキューに入れ、最終的には組み入れ処理でなくスレッドで処理される。スレッドプールによって、C A Sは、より効率よく同時処理を行うことができ、短いロードスパイク下で動作を向上させる。R P C呼び出しはタグ付けした後に解放できるスレッド安全メモリを割り付ける必要があるが、その理由は、R P C移送がそれらを送信し終わるまではバッファは解放できないからである。C A Sは、スレッドIDによりメモリを消去できる再使用可能C ++メモリプールクラスを用いる。

【0106】

C A Sは、ウェブサーバのようなステートレス（原語：stateless）サーバとして実現してもよい。ステートレスサーバは、より多くのサーバ計算機を配置し且つ入ってくる接続を、これらサーバに分配する「総当たり式」ソフトウェアを用いて容易に拡大できるという利点がある。これは、S C D Pクライアントの後の要求が、それが元々接続したサーバの所に行く必要がないからである。C A Sは、要求間に接続ソケットT C Pストリームを維持し、移送セッションキーなどの情報が取り付けられるようにする。この接続が切られると、C A S L I B 3 2は別のC A S処理にも再接続を試みるので、状態をC A S L I B 3 2に又はデータベースの中にプッシュするのが好ましい。

【0107】

処理量を増やすために、C A Sは、活動状態にある複数データベース接続のプールを用いるように設計されている。サーバスレッドはプールから接続を要求し、データベースの接続待ち時間を最小化するため、必要に応じて背景で不動作接続を再接続する。データベース接続プールは再使用可能C ++クラスとして実現されている。C A Sは、D B O j e c tと呼ばれる抄録データベース・インター

フェースを用いるが、このインターフェースは再使用可能C++クラスとして実現されており、CASの他のデータベースへの移植を容易にする。

【0108】

RAFTトークン

SCDPシステムの安全モデルを全般的に向上させるため、CASは、SCD Pクライアントに署名済みRAFT許可トークンを与える。このRAFTトークンは、特定のSCDPクライアントが特定のURNに所定の時間アクセスするのを許可する。CASは、標準化された公開鍵デジタル署名アルゴリズムを用いてRAFTトークンにデジタル署名する。RAFTサーバの実行可能なコンテンツにアクセスするためには、RAFT・VxDはそのトークンをそのサーバに渡さなければならない。RAFTサーバは、CASのデジタル署名を検証し、その後、トークンのコンテンツを検証する。RAFTトークン800は、CASの管理ドメイン内の如何なる数のRAFTサーバに対しても有効で、言い換えれば、広域サービスプロバイダは自己のネットワーク上に複数サーバをインストールでき、RAFTトークンはそれらの何れにも受け入れられることとなる。

【0109】

図示した実施例では、RAFTトークンは、図8に示した形式を備えたデータ構成で実現されている。RAFTトークン800は、URN、URN長804、開始時間806、終了時間808、IPアドレス810、及びCAS署名812を包含する。URN802及び付随した長さ804は、RAFTトークンがアンロックする特定のタイトルを定義する。開始時間806及び終了時間808はトークンの寿命を定義する。このURNの形式は既に説明した。RAFT許可トークンは、RAFTクライアントのIPアドレスをネットワークのバイト順に32ビット値として含む。このトークンは更に、要求されたURN及び32ビット開始及び終了時間も含む。こうした時間は、POSIX1003.1-1988に「新時代の始めからの秒数」又は概ね1970年1月1日、グリニッジ平均時00:00:00からの秒数として定義されている。RAFTサーバが真正確認できるように、CASはCASグループの専用キーでトークンに署名する。RAFTサーバは、サーバの現在時間がトークンの時間帯に入っていなければ、アクセ

スを拒否する。IPアドレスはアクティベータ／トークンを要求するSCDPクライアントのネットワークアドレスを定義する。トークンを提出したSCDPクライアントが同じIPアドレスを持っていなければ、RAFTサーバはアクセスを拒否することで、他のクライアントが不正入手したトークンの使用を防止する。

【0110】

RAFTトークンはアクティベータの一部としてクライアントに送信される。RAFTトークンはアクティベータと共に更新される。アクティベータは寿命制限メカニズムに基づき構成されている。SCDPクライアントは、RPC機構を介してCAS要求を出し、現在のアクティベータが無効つまり満期になる前にアクティベータとトークンのペアを更新する。

【0111】

ランダムアクセスファイル移送プロトコル及びサーバ

図10は、RAFTサーバ1000及び付随したデータベース1050のブロック図を概念的に示す。図示した実施例では、RAFTサーバ1000はPOSIX.1(米国電気電子学会標準1003.1, 1988)と互換性のあるプラットフォーム上で実行可能なアプリケーションとして(例えば、カリフォルニア州パロアルト所在のサンマイクロシステムズ社が市販するサンソラリス(Sun Solaris(商標))オペレーティングシステム又は、レッドハットソフトウェア社が市販するリナックスオペレーティングシステム)として実現してもよく、こうしたプラットフォームは図1に示したものと類似のコンピューターアーキテクチャ上で実行できる。

【0112】

RAFTサーバはRAFTアプリケーション1002及びオペレーティングシステム上で実行されるシンプルネットワーク管理プロトコル(SNMP)マスター/エージェント1004として実現できる。SNMPマスター/エージェント1004を実現するのに適して市販品は、SNMPリサーチイング社から入手できるエマネートがある。マスター/エージェント1004はSNMP標準に従った公開済みのアプリケーションプログラムを用いてネットワーク205と通信する。

【0113】

RAFTアプリケーション1002は、POSIX（ポータブル・オペレーティングシステム・インターフェース標準）ファイル出入力モジュール1006、ファイルシステムインターフェース1008、SNMP計装モジュール1010（つまりRAFT・SNMPサブエージェント）及びネットワーク/RPC/R AFTプロトコル・インターフェースモジュール1012を包含する。

【0114】

SNMP計装モジュール1010は、システム管理者がネットワークの帯域幅を抑えてネットワーク性能を向上させるのに有用な統計的及びロジスティック情報を収集するオブジェクト又は対応するコードを内包している。モジュール1010は、RAFTサーバ1000のオプションの装置である。

【0115】

RPC・RAFTプロトコル1012は、本明細書に記載されたように所有権を主張できるRPCプロトコルを用いてIPに基づいたネットワーク205とのインターフェースをとる。モジュール1012は、このプロトコルを実現し且つRAFTトークンの内容を検証するのに必要なコード及び/又はオブジェクトを含んでいる。

【0116】

ファイル入出力モジュール1006は、米国電気電子学会（IEEE）が発行しているPOSIX標準1003.1に従ったオブジェクト指向で実現してもよい。POSIX・I/Oモジュール1006は、メモリディスク1050にローカル・ファイルシステム・インターフェース抄録を提供する。図10に概念的に示したメモリ1050は、*briq*の形式で複数タイトルを記憶するのに用いられる。本実施例では、解説した **briq**のヘッダ部分と符号化されている **briq**の本体部分は、一緒に記憶される。しかし、これら部分には、モジュール1006及び1008を用いてお互いに独立してアクセスする。ファイルシステム・インターフェース1008は、特定の **briq**に対する要求を受け且つ **briq**が記憶されるメモリ1050中のディレクトリ及びファイル中に **briq**をマップするプログラムロジックを含んでいる。こうした方法で、ファイルシステムイ

ンターフェース 1008 は SCDP システムからのネットワーク要求とメモリ 1050 との間のインターフェースとして機能する。図示した実施例においては、メモリ 1050 は、RAID ディスクアレイ又はディスクファームなどの一つ以上のディスクとして実現してもよい。ファイルシステム・インターフェース 1008 は、ファイル入出力モジュール 1006 とネットワーク・プロトコルモジュール 1012 との間のインターフェースとして機能し、且つ、本明細書で説明しているように、ファイル及び b r i q にアクセスするためのプログラムロジックを実現する。

【0117】

SNMP マスター・エージェント 1004 は、RAFT アプリケーションに埋め込まれているRAFT・SNMP サブエージェントに代わって SNMP プロトコルサービスを提供する。RAFT アプリケーションは SNMP サブエージェントを使って、その管理を遠隔 SNMP マネージャにアクセス可能にする。

【0118】

次の幾つかのステップは、SCDP クライアントとRAFT サーバとの相互作用を説明するものであり、ランチャがタイトルをランチする。ランチャは CAS サーバに連絡して、要求されたURN に対応するURL のリストを入手する。URL は、特定の b r i q の位置（この b r i q が存在するRAFT サーバも含む）を割り出す。各RAFT・URL に関して、最も適切な URL 選択の助けとなるよう、重みを返すようにしてもよい。URL の重み値は高ければ、高いほど好みしい。

【0119】

CAS によるURN-URL 変換について、SCDP クライアントは CAS に、CAS 交換に関する説明で述べたように購入要求を送る。購入要求に応答して、CAS サーバは、SCDP クライアントに、選択したURN のRAFT 許可トークンを含んだアクティベータを与える。許可トークンは選択したURN に関連した複数 URL の何れにも有効である。

【0120】

その後、ランチャは URL のリストを検査して、RAFT・URL が存在する

か判断する。もしRAFT・URLが存在すれば、ランチャはRAFT・URLのリストのみをRAFTアクセストークンと共にARFSD・VxDに送り、ARFSD・VxDはこの情報をRAFTクライアント、つまりSCDPクライアントのRAFT・VxDに送る。ランチャはRAFT・URLのそれぞれの重み付けもする。これらの重みはURN-URL変換においてCASが付けたものとは異なってもよい。RAFTクライアントは、その後、URLリストに指定されたRAFTサーバの何れかと接続を確立する。RAFTクライアントは、URLに付けた重みを用いてどのRAFTサーバに最初に連絡するかを決定するための適切なプログラムロジックをこのクライアント自身に含んでいてもよい。

【0121】

その後、RAFTクライアントは、RAFTサーバ1000上のbriqを開こうとする。このクライアントはプロトコルバージョン、パス名(URLからの)、及びRAFTアクセストークンを特定する。プロトコルバージョンは、RAFTクライアント及びRAFTサーバがプロトコルに関して互換性があるかを確認するのに用いる32ビット値である。アクセスの正当性を確認するため、RAFTサーバは、トークン内のURNがbriqヘッダ内のリストにあるものかを確認する。RAFTサーバ1000は、開ける際にRAFTトークンの開始及び終了時間をチェックする。もしRAFT_OPENが成功すると、RAFTサーバは、RAFTファイルハンドル及び、briqタグのハッシュのようなキャッシュ処理に用いられるbriqの固有IDを返す。

【0122】

RAFTサーバが満期時間を確認するために、RAFTサーバの時間は所定間隔までCASと同期される。したがって、RAFTサーバは現在の時間より早い開始時間は許容し、その間隔の終了まではアクセスを拒否しない。トークン満期時間は、アクティベータ保持時間に、変動するネットワーク及びサーバ待ち時間を加えたものを提唱する。

【0123】

その後のRAFT読みだし要求が出されると、そうした各要求のたびに、RAFTサーバはアクセストークンが満期になっていないかを確認する。RAFTサ

ーバは、該当するクライアントの有効なアクセストークンがなければ、要求を無視する。

【0124】

RAFTアクセストークンはいずれ満期となる。SCDPクライアントのアクティベータ保持機能が、現在のトークンが満期となる前に新しいRAFTトークン入手する責任を負っている。これにより、RAFTトークンが確実にタイミング良く更新され、アクセス失敗は通常の動作条件下では起こらない。RAFTクライアントがRAFT_OPENの間にトークンをRAFTサーバに送ると、RAFTクライアントは開始時間から満期時間までのトークンの有効期間を計算しなければならない。RAFTクライアントはCASの公開かぎなしではトークンの内容の正当性を確認できないので、RAFTクライアントは、このトークンが有効かどうかを確認するのに、更新時間を設定する前にRAFT_OPENが成功するのを待つ必要がある。しかし、更新時間は、RAFTクライアントがトークンを受け取った時間に基づいており、RAFT_OPEN完了時間に基づいてはいない。サーバへの接続を確実に継続するには、RAFTクライアントは、トークン満期時間に先だってCASから新規RAFTアクセストークンを要求する。新しいRAFTアクセストークンを受け取ると、RAFTクライアントは、あたらに入手したトークンと共にRAFT_REFRESH処理をRAFTサーバに送付する。

【0125】

RAFTクライアントがbrinqへのアクセスを完了すると、RAFTクライアントはRAFTファイルハンドルでRAFT_CLOSEメッセージを送る。もしRAFTサーバとRAFTクライアントとの接続が切断されていれば、RAFTサーバはその接続に対応する全ての開いているファイルを自動的に閉じる。

【0126】

RAFTパケットヘッダ定義

RAFTプロトコルに従った全ての通信には、図11に示したようにRAFTパケットヘッダ1100が含まれている。RAFTパケットヘッダ1100は、手順番号データフィールド1102、シーケンス番号データフィールド1104

、パケット長フィールド1106及び状態データフィールド1108を包含するデータ構造体として実現できる。手順番号データフィールド1102はRAFTプロトコルメッセージタイプを特定し、整数形式で実現できる。シーケンス番号フィールド1104は要求に対して応答を一致させるのに用いられ、整数形式で実現できる。シーケンス番号は、一つの接続に関してのみ固有性がある。パケット長フィールド1106は、ヘッダのサイズを含まないパケットデータのサイズを示し、整数形式で実現できる。状態フィールド1108はRAFT要求から状態を示し、整数形式で実現できる。非ゼロ状態は、要求が失敗したこと示す。異なるプロトコルメッセージに対して異なる状態コードが返される。しかし、ゼロ状態は要求が完全に成功したことを示す。非ゼロ状態の場合はパケット長フィールドがゼロに設定され、これは要求が失敗した場合はパケットデータが返されないことを示す。RAFTプロトコルに従って、パケットヘッダにはRAFTパケットデータが続く。

【0127】

RAFTプロトコルメッセージ

RAFTプロトコルは、`briq`アクセス及びRAFTトークン管理を可能にする4つの異なるプロトコルメッセージからなる。TPC接続を確立すると、要求者のプロトコルバージョンを特定するために、最初のRAFTプロトコルメッセージには、その引き数の一つとしてこのプロトコルバージョンが含まれている。RAFTプロトコルメッセージのリスト及び記述は以下の通りである。RAFT_OPEN機能は、プロトコルバージョン、トークン長、RAFTアクセストークン、パス長、及びNULで終わる全パス名で呼び出される。成功すると、RAFTファイルハンドル、RAFT_ID、及びRAFTサーバがサポートする最大読み出し長となる。RAFT_IDを用いてSCDPクライアントキャッシュ・タグを生成できる。失敗が起きた場合に備え、RAFT_IDは、複数RAFTサーバにおける一貫したキャッシュを達成するための`briq·ID`よい。最大読み出し長は、RAFTクライアントにRAFT_READ処理中に要求できるデータ量を知らせるのが目的である。

【0128】

RAFT_REFRESH_TOKEN機能により、RAFTクライアントは新しいRAFTアクセストークンを使ってRAFTサーバを更新できる。この機能はトークン長、RAFTアクセストークン、及びRAFTファイルハンドルで呼び出される。成功すると、新しいRAFTアクセストークンは指定されたハンドルに関連した現在のトークンと入れ替わり、トークンの満期時間を長くする。新しいトークンが有効でなければ、現在のトークンは保持される。この機能はデータを返さないが、ヘッダ内の状態は成功又は失敗を反映するように更新される。

【0129】

RAFT_READ機能は、RAFT_OPEN呼び出しから戻されたRAFTファイルハンドル、64ビット・オフセット及び長さで呼び出される。要求したデータにアクセスするには、RAFTファイルハンドルは、有効なアクセストークンに関連付けられていなければならない。

【0130】

RAFT_CLOSE機能は、開いているRAFTファイルハンドルを閉じるのに用いる。この呼び出しはRAFTファイルハンドルを取り、データは返さない。しかし、ヘッダの状態は成功又は失敗を反映するように更新される。

【0131】

ランチストリング

図9は、本発明によるランチストリング900を示す。図9に示すようにランチストリング900は、URNデータフィールド902、店舗IDデータフィールド904、商品タイプデータフィールド906、加入ドメインデータフィールド908、及び金額データフィールド910を包含するデータ構造体として実現できる。URN902は所望のコンテンツを固有に識別し、更に、本明細書に記載したように実現できる。店舗IDデータフィールド904は特定の店舗ショーウィンドウをECマースシステムに特定し、且つ、数字列、英数字列、又は整数形式で実現してよい。店舗IDは、報告のために異なる店舗ショーウィンドウからの取引を分離するために使われる。複数店舗が本当に同じ組織に属していれば、単一の店舗IDを共有してもよい。商品タイプ906は、取引が加入による購

入かミクロ取引による購入かを示し、且つ、数字列、英数字列、又は整数形式で実現してよい。加入処理は、一回の支払いに特定期間はタイトル又は一組の複数タイトルを無制限に利用するためのものである。ミクロ取引はユーザの借方勘定への請求金額であり、「一回の利用に対する支払い」モデルをサポートするのに用いられる。加入ドメイン908は、当該取引が「今週のホットなゲームパック」や「個人事業用のアプリケーションパッケージ」などの特定の加入オファーを購入する際の対象となっているかを示す。加入ドメインは数字列、英数字列、又は整数形式で実現してよい。金額フィールド910は、ミクロ取引の購入額を示し、整数形式で実現してよい。

【0132】

図14に示したように、ランチストリング900の内容は、Eコマースサーバ・フロントエンドモジュール1408によって生成される。CASは、例えば標準化された公開鍵デジタル署名アルゴリズムを用いてランチストリング900にデジタル署名する。その後は、ランチストリング900はCASグループの専用キーを特定する付加的CAS署名フィールド912を含む。ランチストリングは、SCDPクライアントにEコマースシステムを介してサービス業務の一環として送る。SCDPクライアントは、上述のようにCASとのランチ前の交渉中に、ランチストリングをCASに送り返す。

【0133】

Eコマースシステム

本発明と共に用いるのに適した電子通商ソフトウェアアプリケーション（以下Eコマースシステムと称する）は、マサチューセッツ州ケンブリッジ所在のオープンマーケット社から市販されているトランスクレクト4.0である。Eコマースソフトウェアは、ユーザ勘定を管理し、金融取引を実行するために用いられており、例えば、1) ユーザ勘定情報を管理し、2) 購入及び支払いを管理し、3) クレジットカード情報を収集及び検証し、4) 取引を完了するために用いられる。

【0134】

図2を再度参照すると、Eコマースサーバ202は、図1を参照して説明した

ものと類似のコンピュータアーキテクチャ上を走るサーバアプリケーションを包含する。このアプリケーションは、サン社のソラリスなどのオペレーティングシステム又はサーバタイプのアプリケーションを実行するよう設計されたその他のオペレーティングシステム上で動作するよう設計されている。図14を参照すると、Eコマースサーバ14は、オペレーティングシステム1404が走るハードウェアプラットホーム1402を包含する。実際のEコマースサーバアプリケーション1406は、フロントエンドモジュール1408及びバックエンドモジュール1410をSCDPシステム200のその他の様々な構成要素に提示する。具体的には、サーバ1400のフロントエンドモジュール1408は、ウェブサーバ・フロントエンドをSCDPシステム200に対してネットワーク205を介して提示するように実現できる。こうしたフロントエンドは、現在インターネット上に存在する他のウェブサーバと似たものである。サーバ1400のバックエンド410は、請求書作成データベース204とのインターフェースを取り、データベースの問合わせと、交渉及びタイトルの購入に関連した取引及びクロ取引の実行とに必要なロジック及び／又はオブジェクトを実現する。上述のように、Eコマースサーバ1400は、専用LAN又はインターネットなどの広域ネットワークを介して、銀行やクレジットカード調査及び電子貸方記入などのサービスを行う第三者信用貸し処理サーバに接続できる。サーバ1400のフロントエンドモジュール1404及びバックエンドモジュール1410は、共通ゲートウェイインターフェース(CG1)規格に従って書かれた一連のスクリプトを介して通信する。通常の技能を備えた当業者にとっては、他の市販のEコマースサーバアプリケーションをここに述べたもの以外にSCDPシステムと共に使用可能であることは明白であろう。

【0135】

データベース204はサーバ202に付随しており、従来のシリアルデータベースを包含してもよく、取引を進めるのに必要な信用貸し及び請求書作成情報を記憶するのに用いられる。

【0136】

サーバ1400のフロントエンドモジュール1408は、図9を参照して更に

詳しく説明したようにランチストリングを生成するのにコード又はオブジェクトを更に包含する。一旦生成されると、ランチストリングはデジタル署名のためにC A Sサーバに送られる。

【0137】

図示した実施例では、Eコマースシステムはサーバ及び店舗ショーウィンドウを包含し、この両者が協力して、ユーザがカタログ内を移動できるようにし、購入情報を受付且つ承認する。Eコマースシステムは、外部構成要素と対話するのにオープンウェブに基づくアーキテクチャを用いる。本発明のS C D Pシステムソフトウェアモジュールは、URLをEコマースソフトウェアのウェブサーバフロントエンドに通知することで、Eコマースソフトウェアと通信する。この通知に応答して、トランSACTIONはURLで符号化された特定の引き数でC G Iプログラムを呼び出す。C G I呼び出しを介してURLを評価すると、トランSACTIONソフトウェアがデータベースの状態を変更する。処理シーケンス全体は、単に一組のURLを評価することで終了する。Eコマースシステムは、ユーザ勘定又はクレジットカード情報などのクライアントデータを捕捉し且つ保持する。

【0138】

Eコマースシステムが、店舗ショーウィンドウに商取引能力を与え且つウェブを介したクレジットカード取引を実行する能力を備えた機能を完備したシステムであれば、C A SとEコマースシステムとの対話は主に3つの異なる場所で行われる。ユーザがタイトルを購入すると、ユーザは、サービス業務URLと呼ばれるリンクをその上に含んだ「デジタル領収書」と称するページを受け取る。このサービス業務URLは、実際は、C A Sからランチストリングを入手するのが目的のC G Iプログラムである。後に更に詳しく述べるように、ランチストリングは、C A Sが後にユーザのソフトウェアに対する権利を確認する共にEコマースシステムと処理を終了するために必要な全情報の集まりである。この情報はC A Sのみが理解できる形式で返され、C A Sは後にそれ自身のランチストリングを検査する。ランチストリングをクライアントのブラウザに返すと、ブラウザがS C D Pクライアント内部でランチャを起動し且つランチストリングをランチャに回す。後に、ランチャはランチストリングをC A Sに送って、アクティベータを

要求できる。CASはランチストリングを検査して、もし当該購入が決定していれば、成功するかを確認することをEコマースサーバに要求する。しかし、CASはまだこの取引を成立させない。この時点では、CASはアクティベータをランチャに返して、タイトル実行が開始される。最初のアクティベータの寿命は短く設定されている。例えば、最初のアクティベータが満期になる直前に、SCDPクライアントVxDがランチャに通知して、CASにアクティベータを更新するよう要求する。アクティベータの第1回目の更新が実行されると、CASLIB32が再度ランチストリングを提供し、今回はCASはEコマースサーバとの間で取引を完了する。取引の完了を延期することで、請求書作成の前にタイトルがSCDPクライアント計算機で正しく実行されていることをSCDPシステムが間違いなく確認できる。

【0139】

SCDPシステムは5つの異なる購入モデルをサポートする。最初の購入モデルの「タイトル加入」では、所定の時間は特定タイトルへの無制限のアクセスができる。「アーケードゲームパック」などのパッケージ加入である第2購入モデルは、限られた時間内に一組の複数タイトルに無制限のアクセスを提供する。こうしたパッケージ加入に含まれるタイトルセットは時間が経つと変わることもある。例えば、ユーザが「ホットな新しいゲームパック」への加入を購入したとすると、このパッケージで利用できるタイトルは当初の加入購入から一週間から二週間経つと変わることもある。「1回の使用毎の支払い」の第3購入モデルは、時間無制限で一度だけのアクセスを提供する。「時間に基づく請求」の第4番目の購入モデルでは、ユーザはタイトル実行時間に応じて料金を請求されるか、特定の時間ブロックを購入できる。「月払い」の第5番目の購入モデルでは、SCDPシステムは既存のマルチサーバオペレーション(MSO)又は電話会社の請求システムに組み込まれ、料金を顧客の日々の請求書に加算する。細かな変更点を含んだこれ以外の購入モデルを加えることもできる。

【0140】

仮想店舗ショーウィンドウ

仮想店舗ショーウィンドウサーバ215及び付随のデータベース213は、S

CDPシステム200のクライアント及び将来のクライアントに仮想カタログを提示する。図示した実施例では、サーバ215は、例えばサーバハードウェア上で実行されるオペレーティングシステム上で実行されるサーバアプリケーションなどの従来のウェブサーバとして実現でき、Eコマースサーバ202に関連して説明したものと類似のものでよい。店舗ショーウインドウアプリケーションは、一連の品揃えをクライアントが通常のネットワークブラウザで検索できるように表示するグラフィック・ユーザインターフェースを含む。こうした品揃えは特定タイトル名、タイトルの簡単な説明、要する費用又は購入の選択肢を含み、映画やオーディオクリップなどのマルチメディアタイトルの場合は、タイトルコンテンツの短いサンプルなどを含んでいてもよい。更に、各タイトル選択対象には対応するURNが付随している。店舗ショーウインドウは、データベース213と対話する適切なデータベース問合わせエンジンを実現する。尚、データベース213には、タイトル、説明、料金、デジタルオッファー、及びURN情報をSCDPシステム200内の大量のタイトルに関して記憶することができる。特定タイトルが選択されるとそれに応答して、店舗ショーウインドウアプリケーションのロジックが該当するURNに関してデータベース213に問合わせを行い、本明細書に記載した方法で適切な情報をEコマースサーバ202に送る。

【0141】

図示した実施例では、上述したように、仮想店舗ショーウインドウサーバ215及びデータベース213は、専用の安全なローカルエリアネットワーク205を介してキャッシュサーバ210に接続されている。しかし、SCDPシステム200は、ローカルエリアネットワークを介するのではなく、例えばインターネットなどの広域ネットワークを介してキャッシュサーバ210及びEコマースサーバ202に当業者に理解できる方法で接続された1つ以上の仮想店舗ショーウインドウを用いて実現できることは、通常の技能を備えた当業者には明らかであろう。こうした実現例は店舗ショーウインドウサーバは公共ネットワーク上に位置するが、様々な情報の部分集合が将来のクライアントの目に触れる可能性がある。例えば、加入料金を支払うクライアントは、タイトル及び関連する購入選択肢に関して最低の情報しか提供しないかもしれない公共ネットワーク上の店舗ショ

一ウインドウサーバにアクセスする一般大衆よりも、大量の情報及び／又はタイトルデータのサンプルを提供する専用ネットワーク上の店舗ショーウインドウサーバにアクセスするかもしれない。

【0142】

b r i q 形式

図12は、本発明によるb r i q 及びその構成要素のブロック図を概念的に示す。図示したように、b r i q 1200は、b r i q ヘッダ1202、暗号ブロック1204、スーパーブロック1206、及び1つかそれ以上のタイトル1208A乃至1208Nを包含する。b r i q ヘッダ1202は、システム登録情報、解像度、アプリケーションタイトル、及びURLなどの、SCDPクライアント内のランチャモジュールが使う情報を含む。暗号ブロック1204は、タイトルが符合化されているか、そもそもしそうならその符号化に用いられた暗号キーバージョンを特定するためにSCDPクライアント内のARFSD・VxDが用いる。スーパーブロック1206は、b r i q サイズ、作成データ、ルートディレクトリが存在するエントリなどのb r i q に関する一般的な情報を含むことが可能である。タイトル1208A乃至1208Nは、それぞれ1つのディレクトリ及び特定のタイトルに関連した1つ又はそれ以上のファイルを含むことができる。本明細書で説明したように、b r i q はRAFTサーバに記憶し、RAFTプロトコルを用いてSCDPクライアントによって遠隔アクセスされ、ローカルファイルシステムとしてホストのオペレーティングシステムに提示される。

【0143】

本発明によれば、一つ又はそれ以上のタイトルが、図12を参照して説明したように、b r i q 形式で処理及びパッケージ化される。タイトルをb r i q 形式にする処理は以下の通りである。第1に、ウインドウズ(R)のオペレーティングシステム内のビューアユーティティのようなユーティティツールを用いて、タイトルからレジストリ情報抽出する。こうしたレジストリエントリは、ファイル名、ディレクトリ名、及びコンフィギュレーション引用などの特定タイトルを実行するのに必要な最小限の情報セットを包含できる。抽出したレジストリエントリはファイルに入れられる。次に、これらレジストリエントリを含んだファイ

ルを作成者プログラムに提供する。本実施例では、作成者プログラムは、タイトル及びレジストリエントリを包含するデータを取って、こうした情報を現在利用可能な多くの暗号化アルゴリズムの何れかに従って暗号化する機能がある。結果として生成される暗号化ファイルは、図12のディレクトリ1208A乃至1208Nに示したように、従来のディレクトリ階層に記憶される。次に、このファイルシステムのルートディレクトリ及びこのファイルシステムのサイズなどを含んだ付加的メタ情報は、図12に示したようにbriq1200のスーパー区块1206に記憶される。次に、briq内の暗号化情報を解読するのに必要な暗号キーに関する情報は、暗号区块1204に記憶される。暗号区块1204内の情報は、キーバージョン及び使用された暗号タイプの記述を特定するデータを包含できる。briq・URL及びシステム要件などの情報は、実行可能ファイル及びタイトルの名前、ネットワークドライブ及び付加的タグのマップと共にbriqヘッダ1202に入れられる。図12に示したように、briqヘッダ1202に含まれる情報は暗号化されない。

【0144】

アクティベータ

アクティベータは図13に示したような形式を備える。具体的には、アクティベータ1300は、トークン1302、許可データ1304、暗号キー1306、及びオプションで1つかそれ以上のバイトコード1308乃至1312を包含する。図示した実施例では、トークン1302は、図8に関連して説明したRAFTトークン800に類似のものでよい。許可データ1304は、CASサーバから新しいアクティベータを要求する際にSCDPクライアントが使用する「保持」データを包含する。こうした許可データは、単純な数値列又はコードで実現してもよいし、更に、クライアントに前もって関連づけられたデータのハッシュのようなより洗練された高度な実現例でもよい。キー306は、briq内に含まれたデータを、実行前に解読するのに有用な暗号データを包含する。暗号データを含む解読キー306は、briqデータ解読に役立つ、バイトコードインターフィラ308が抽出し且つRAFT・VxDに送られるビット列を包含できる。

【0145】

単純な実施例では、アクティベータ1300は、トークン1302、許可データ1304、及びキー1306のみを包含する。より高度な実施例では、1つ又はそれ以上のバイトコード1308乃至1312が含まれる。図示した実施例においては、バイトコードは実質的に、バイトコードインタプリタ308として実現されている物理又は仮想計算機の何れかで実行可能な命令群である。図示した実施例においては、バイトコードインタープリタ308は、アクティベータから送られたこうしたバイトコードを実行する能力のある仮想計算機を包含する。アクティベータ1300で使用可能なバイトコード1乃至Nの種類及び性質は後に説明する。バイトコードインターパリタ308は図3Cを参照して説明してある。

【0146】

コード曖昧化

プログラムの核心部はフロー及び基本命令に分解できる。通常は、フローは、基本命令からより高いレベルの抄録を構築することも含む。最適化には、冗長基本命令を結合すること、フローを配列し直して類似の構造体を結合して除去すること、及びパターンを認識してそれらをより効率的なパターンと交換することが含まれる。最適化により、元々の仕様書の指定に従ってプログラムの動作が維持される。曖昧化処理により1つ以上の正しい結果が得られることもある。無作為に選択するのではなく、正しいバリエントの全体又は部分集合を並列に生成すれば、個別生成にはコスト高になるが全体的にはより効率的になる。

【0147】

一般的には、最適化には、問題に対する解決策を見つけ、よりよい解決策を得るためにそうした解決策を改良することが含まれる。実際のコンパイルに当たっては、高レベルコードの単純に生成された正しい表現式を、その正確性を維持しつつより効率的なコードに変換することを意味する。最悪化もこの正確性を保持できるが、曖昧化形式の逆コンパイルが困難なので効率が犠牲になる。

【0148】

フロントエンドとアセンブラーを分離することで、異なるレベルにおいて最悪化子（原語：pessimizer）を挿入でき、且つ最悪化において高度の柔軟性

を提供する例えばLisp/Schemeのような他の高級言語を後から使用できる。多くの最悪化手法を本発明で使用できるが、それには、1) バイトコードストリームをローカル再整理し且つ曖昧化するアセンブラーレベルピープホール最悪化子、2) 一定の構造的最悪化に対しより自然なインターフェースを提供する、高級言語とアセンブラーとの間の翻訳レイヤを曝す中級言語最悪化子、3) 高級言語コードに総称(原語: generic)処理を実際にを行う代わりに、ある機能を表現する複数の方法をコーダに指定させ、その後、コーダがコンパイラに既に開始された選択肢の組合せ論的拡張を備えた形式を直接生成させるような、高級マニュアル最悪化子が含まれる。

【0149】

理論的には、誰かがアクティベータをシングルステップして、アクティベータの行う変更を監視して、`breq`の解読法を発見したり、更に単純には、`briq`が解読されたら停止して、メモリからクリアテキストをダンプすることも可能である。翻訳困難な「曖昧化」手法で書かれた、異なるバイトコードシーケンスを用い、且つ合い鍵のような同一物を再使用する事を避けることで、本発明は人間の逆コンパイラの作業を困難にし、自動解析を不可能にする。バイトコードにより、権限を持たないクラッカーの1度のダウンロードに対する作業を任意により時間の掛かるものとし、それが他のダウンロードには利用できないようになる。

【0150】

本発明のアクティベータに有用な曖昧化手法の例には次のようなものがある。

- ・処理毎に大量のアルゴリズムの中から選択して、同一オブジェクトに対する2回目の要求にもコードが大きく異なるようにする。
- ・例えばコンパイラ最適化手法を用いて、動作維持処理をバイトコードに直接適用する。
- ・SCDPクライアントに複数のバイトコードセットをサポートさせるか、バイトコードリスト自身を暗号キーさせる。
- ・自己修飾バイトコード。
- ・「トラップドア」バイトコードストリーム(例えばバイトコードシーケンスを

生成する) 及び部分集合を拾い出してバイトコード主体を有用なアルゴリズムにマップするマップ関数。制約条件を定義して、その後、役立つシーケンスをスペース中で探す必要があるかもしれません。

・存在するコードにパターンによって関連する可能性のある、注意を逸らすものとしての「デッドコード」バイトコード。

・一定のバイトコードを使用しない。例えば、コードは後続の実行では意味が異なる。(高級ツールは作業アルゴリズムに割り込んでこれらを生成できる。この延長上には、特定の位置又はレジスタを参照する如何なる命令も使用しないことが含まれる。)

・暗号具体例で用いられる「単項」演算子。

・バイトコードのパラメータ(例えば、使用頻度、非相關要素など)に基づいてそのコードのマッピングを最適化する。

・暗号をバイトコードに直接具体化する際に、部分キー／スケジュールまたはコードシーケンスを引き渡して、「標準」形式のキーでないキーを生成する。

・後のコールバックで追加バイトコードをバイトコードにダウンロードさせるか、サーバにバイトコード変更を非同期的に送信させる。

・現在の環境データを、バイトコード、データ、キーイングデータ、`b r i q` そのもののような弱いエントロピー又はその環境内のその他の2進数、又はダウンロードしたバイトコードのソースとして使用する。

【0151】

実際に曖昧化したものは、それらがどのように互いに組み合わされるのか、又はどうやってそれらを処理するのかについての情報を与えるフレームワーク内に生成され得るのが理想的である。

【0152】

テクニック(技法／手法)

アクティベータの強度を上げるもう一つの方法は、アクティベータを不完全にして、アクティベータがCASと追加連絡しなければ動作を継続できないようにすればよい。「テクニック」とは、CAS内部で実行し且つ要求をサポートするためにカスタマイズした一片のコードである。複数のテクニックを用いてもよい

が、単一のテクニックである種類に属する複数アクティベータには十分である。単純なテクニックは、CAS内部にハードコード化して実現したり、動的にロードされたバイトコード又は共有オブジェクトで実現できる。テクニックプロトコルにするアクティベータは、SCDPクライアントからの移送用の存在するRPC上のレイヤとし、テクニックが定義済みメッセージを備える手間を省くことができる。本発明では、アクティベータバイトコード及びテクニックバイトコードは別の言語として扱うことができる。テクニックコードは、暗号ルーチン全体用の単一バイトコードを単に備えていればよい。

【0153】

本発明のアクティベータ内に曖昧化バイトコードを実現するためには、次の構成要素を用いる。1) バイトコードインターフリタ、2) バイトコードアセンブラー、3) 暗号バイトコードルーチン、4) 有益な地点でアクティベータにコールインするARFS・VxDへのインターフェース、5) アクティベータがCAS内の具体化されたテクニックと通信できるようにする、本明細書で述べたプロトコル、6) CASアクティベータ製造機能（アクティベータファクトリ710）。

【0154】

本明細書に説明されたシステムは、専用インターネットだけでなく広帯域ネットワーク上でもコンテンツのオンデマンドでの安全な引き渡しを容易にすることが分かるであろう。

【0155】

こうして説明した本発明は、ソフトウェアのみ、ハードウェアのみ、又は専用ハードウェアをサポートするためにファームウェアの形式で記憶されたプログラムコードを含んだハードウェアとソフトウェアとの組合せで実現してもよい。上述の実施例の一つのソフトウェア実現例は、図1のディスクケット142、CD-ROM147、ROM115、又は固定ディス152などのコンピュータ読出し可能媒体のような有形媒体に固定された一連のコンピュータ命令又は、モデム又は他のインターフェース機器（例えば、媒体191を介してネットワーク195に接続された通信アダプタ190）を介して搬送波でコンピュータシステムに通

信可能な一連のコンピュータ命令を包含できる。媒体191は、光通信又はアナログ通信回線を含むがそれには限定されない有形媒体でもよいし、マイクロ波、赤外線、又はその他の通信手法を含むがそれには限定されないワイヤレス技法を用いて実現してもよい。これらの一連のコンピュータ命令は有形媒体に含まれていても搬送波に乗っていても、本発明に関連して既に説明した機能の全て又は一部を具現化するものである。通常の技能を備えた当業者であれば、こうしたコンピュータ命令はコンピューターアーキテクチャ又はオペレーティングシステムで用いられる多くのプログラミング言語で書くことができ、又、機械実行可能な形式で存在可能であることが理解できるであろう。更に、こうした命令は、半導体、磁気、光学、その他のメモリデバイスを含むがそれに限定されない、現在又は将来のメモリ技術を用いて記憶させてもよいし、マイクロ波、赤外線、又はその他の通信手法を含むがそれには限定されない現在又は将来の通信技術を用いて送信してもよい。こうしたコンピュータプログラムは、印刷文書又は電子文書（例えば、システムROM又は固定ディスク上にコンピュータシステムを予めロードした収縮包装したソフトウェア、又は、インターネット又はWWWなどのネットワークを上でサーバ又は電子掲示板を介して販売する）を付けて取り外し可能媒体として販売することも考慮されている。

【0156】

本発明の様々な例示的実施例を開示してきたが、通常の技能を備えた当業者には、本発明の精神及び範囲から逸脱することなく本発明の利点の一部を提供できる様々な変更及び修正が可能であることは理解できるであろう。通常の技能を備えた当業者には、同一の機能を持った他の構成要素を適切に用いることが可能ることは明白であろう。更に、本発明の方法は、適切なプロセッサ命令を用いて全てソフトウェアから具体化することもできるし、ハードウェアロジック及びソフトウェアロジックを組み合わせて用いたハイブリッドとしても具体化して、同様の効果を得ることができる。

【0157】

以下に特許請求の範囲を記載する。

【図面の簡単な説明】

本発明の上記並びに他の特徴、目的及び利点は、添付図面と併せて下記の詳細な説明を参照することで更に良く理解されるであろう。

【図1】

本発明で使用するのに適するコンピュータシステムのブロック図である。

【図2】

(A) 本発明のコンテンツの安全な引き渡しシステムを実行することができる広帯域ネットワークの概念ブロック図である。

(B) 本発明のシステムの要素及び本発明による、他のネットワークの要素との相互作用を示している概念ブロック図である。

【図3】

(A) 本発明によるSCDPの概念ブロック図である。

(B) 図3AのSCDPクライアントのランチャモジュールの概念ブロック図である。

(C) 図3AのSCDPクライアントのARFS・VxDモジュールの概念ブロック図である。

(D) 図3DのSCDPクライアントのRAFT・VxDモジュールの概念ブロック図である。

【図4】

(A) 乃至(B) 本発明による、コンテンツへの加入手順及びタイトルのランチ手順を示すフローチャートを合わせて示す。

【図5】

(A) 乃至(C) 本発明による、SCDPクライアントによって実行される手順を段階的に示すフローチャートを合わせて示す。

【図6】

本発明による、SCDPクライアント構成要素によって実行される手順を示すフローチャートである。

【図7】

(A) 本発明による図2のCASサーバの概念図である。

(B) 本発明による、CASサーバによって実行される手順を示すフローチャ

ーである。

【図8】

本発明によるR A F Tトークンの概念図である。

【図9】

本発明によるランチストリングの概念図である。

【図10】

本発明による図2のR A F Tサーバの概念図である。

【図11】

本発明によるR A F Tパケットヘッダの概念図である。

【図12】

本発明によるb r i qデータパッケージの概念ブロック図である。

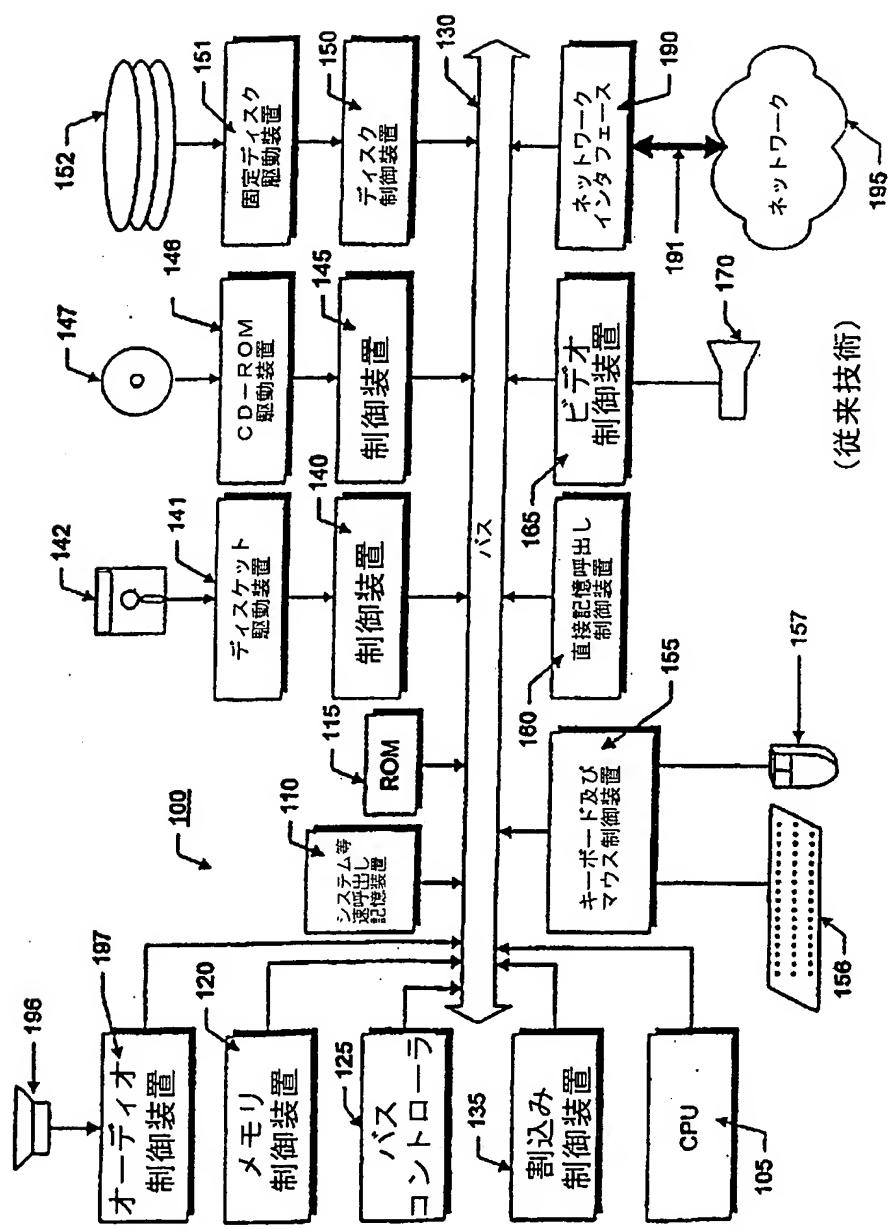
【図13】

本発明によるアクティベータの概念ブロック図である。

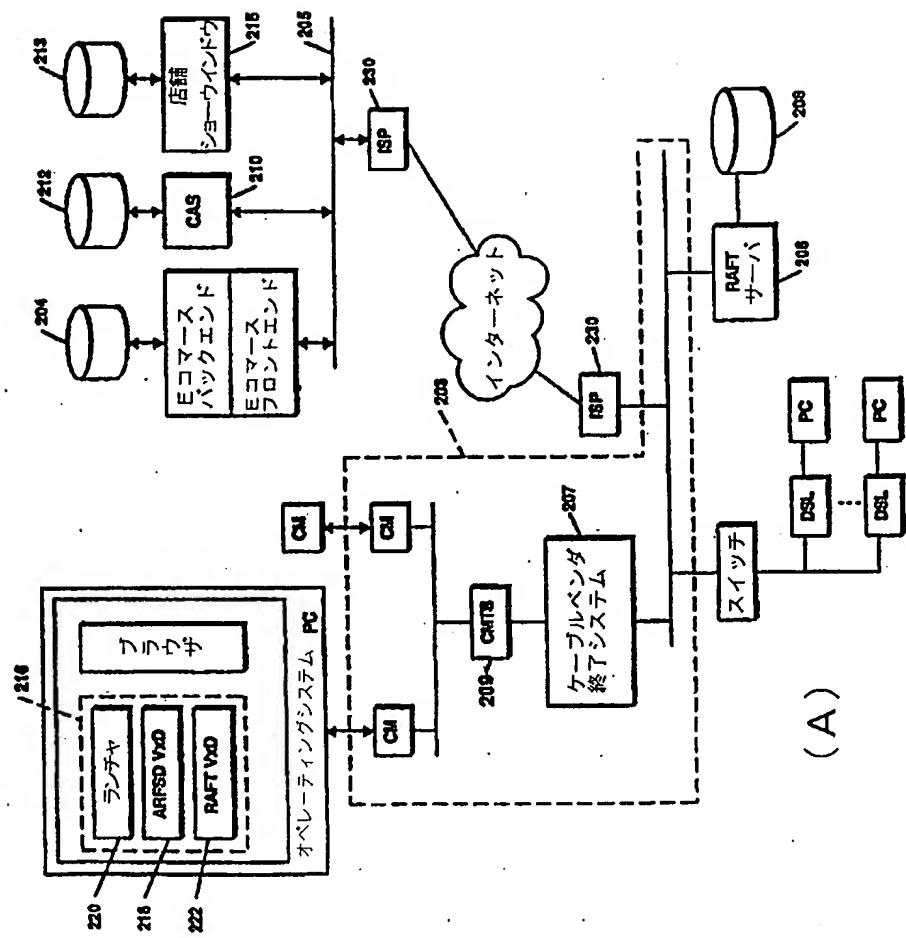
【図14】

図14は、本発明によるEコマースの概念ブロック図である。

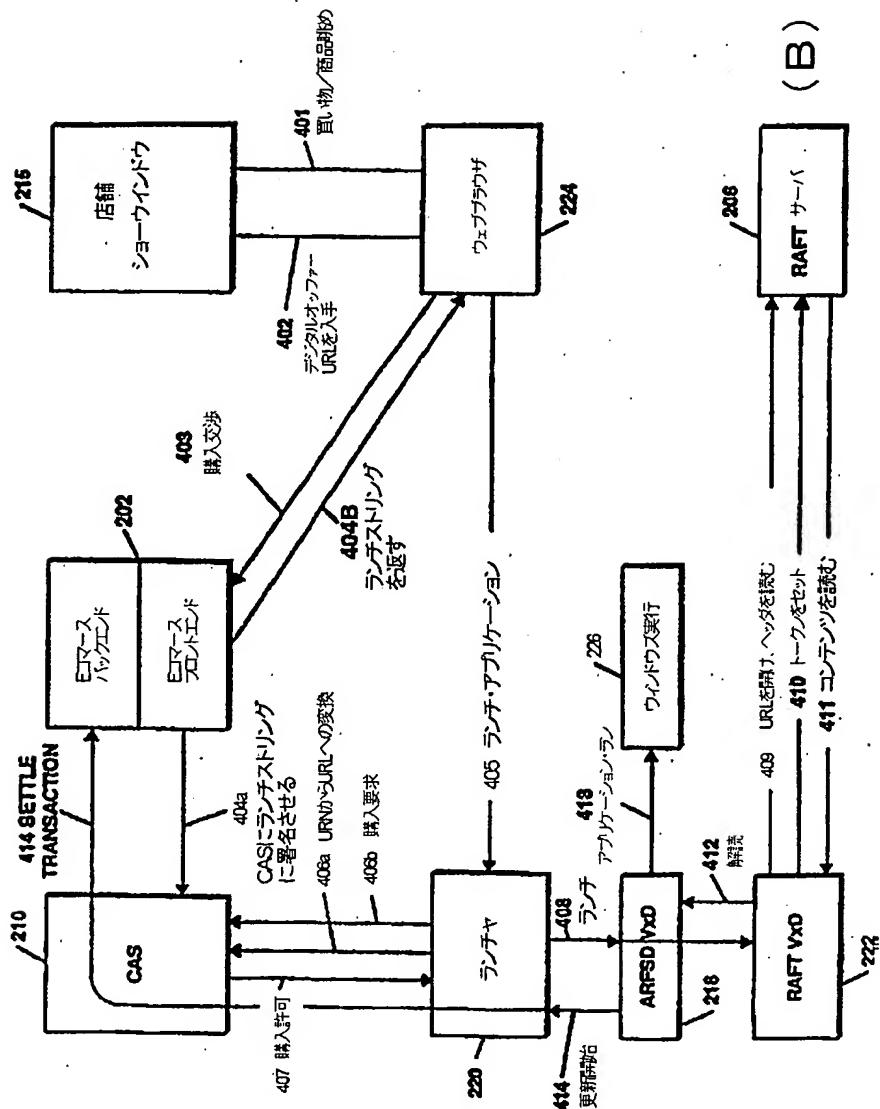
【図1】



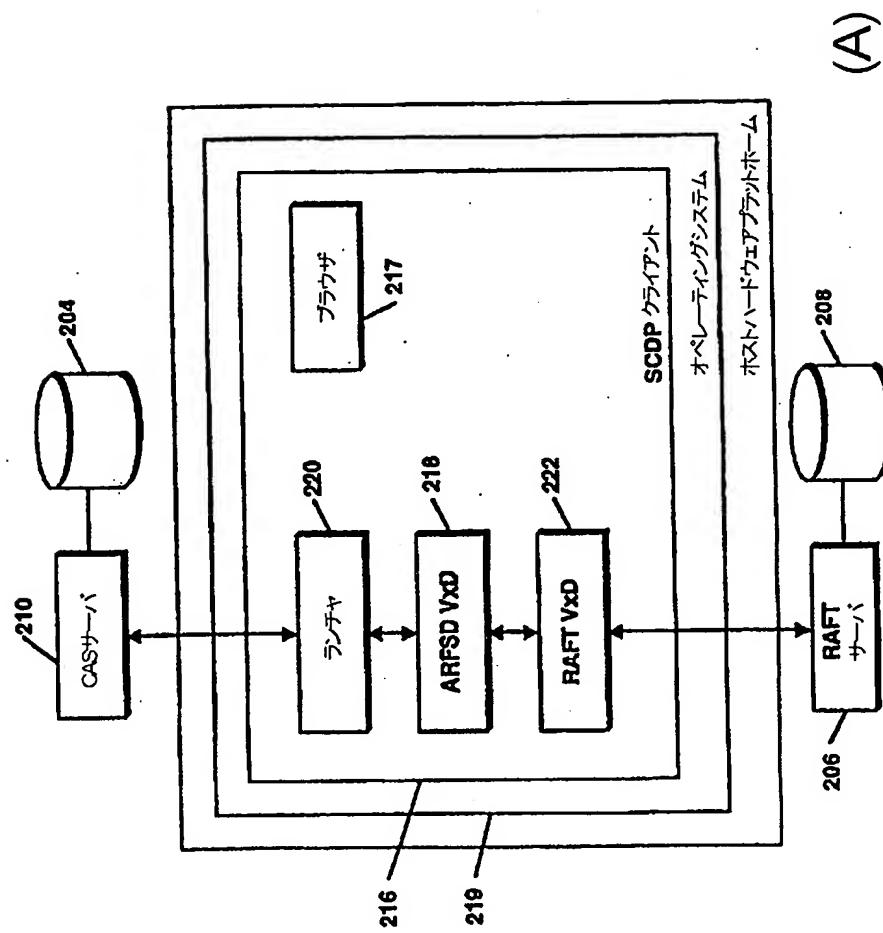
【図 2 A】



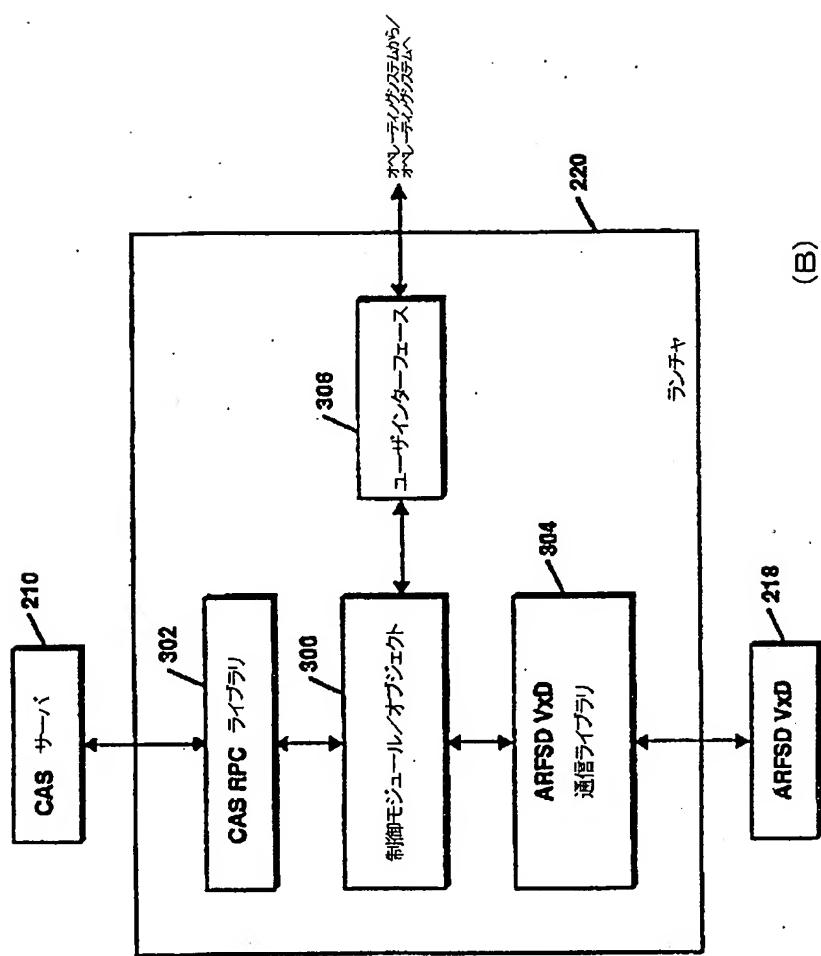
【図2B】



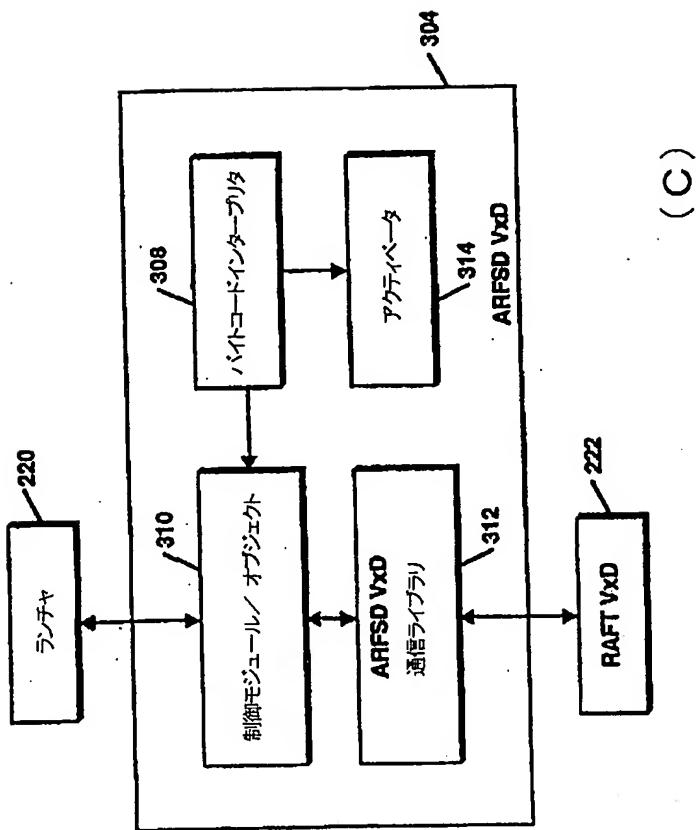
【図3A】



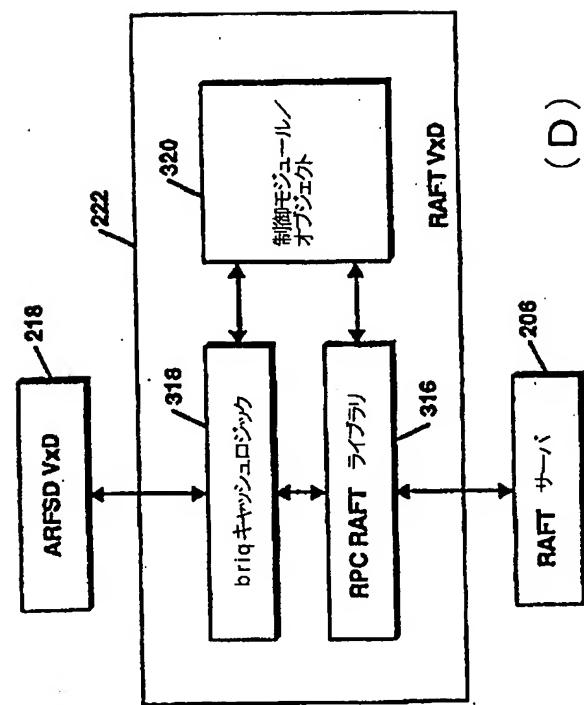
【図3B】



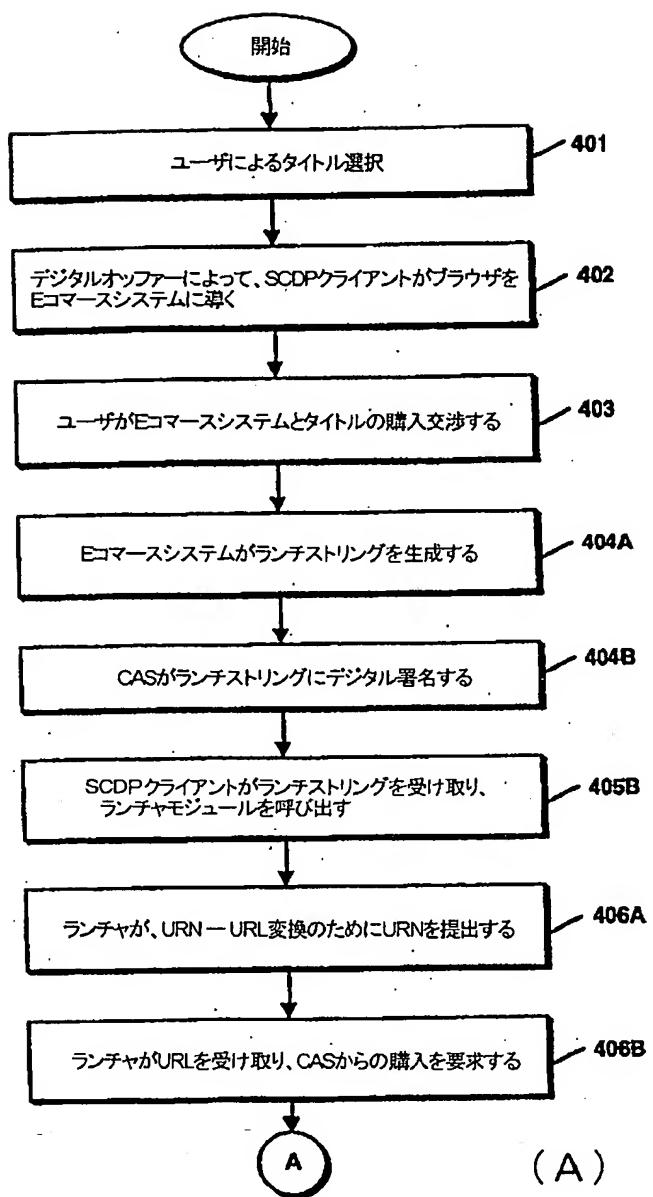
【図3C】



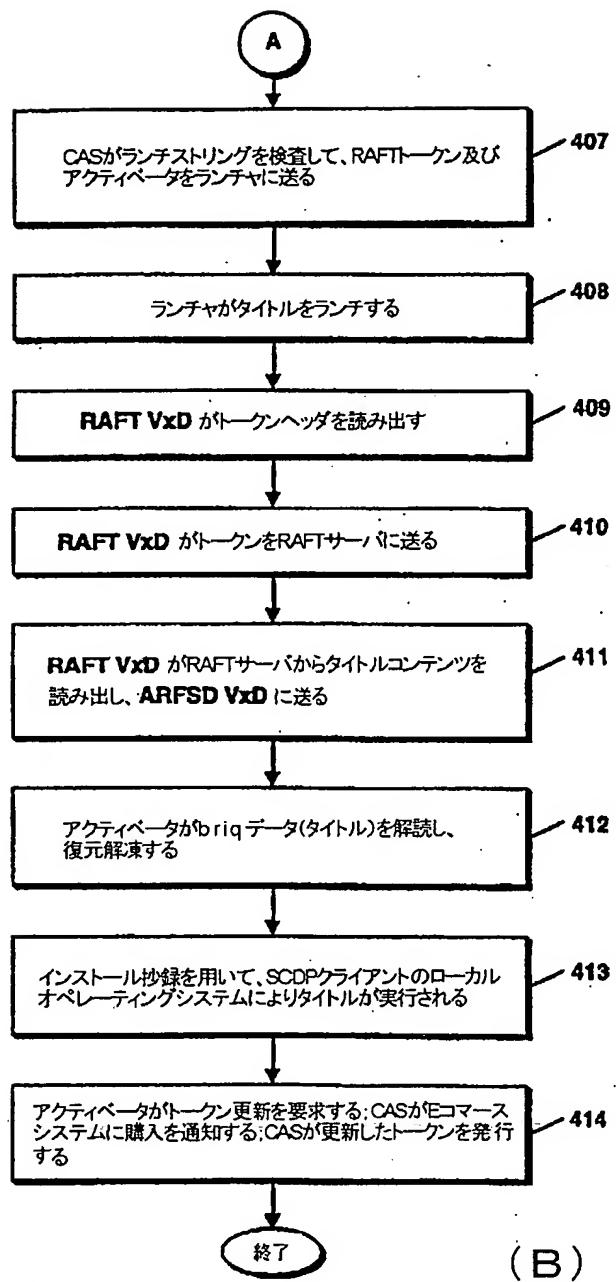
【図3D】



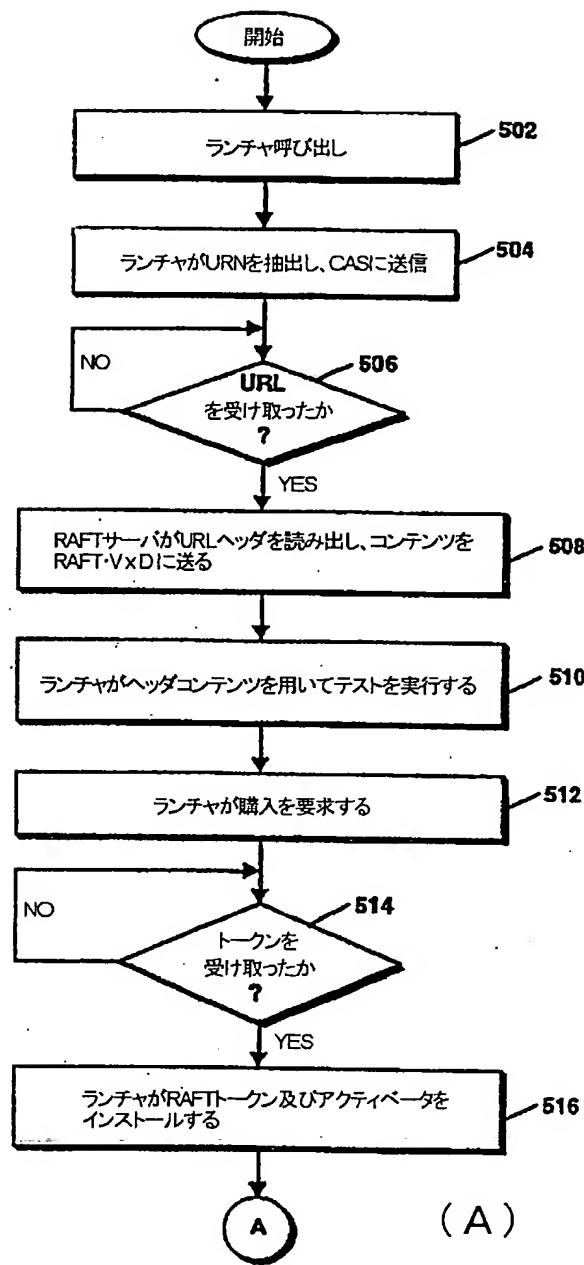
【図4A】



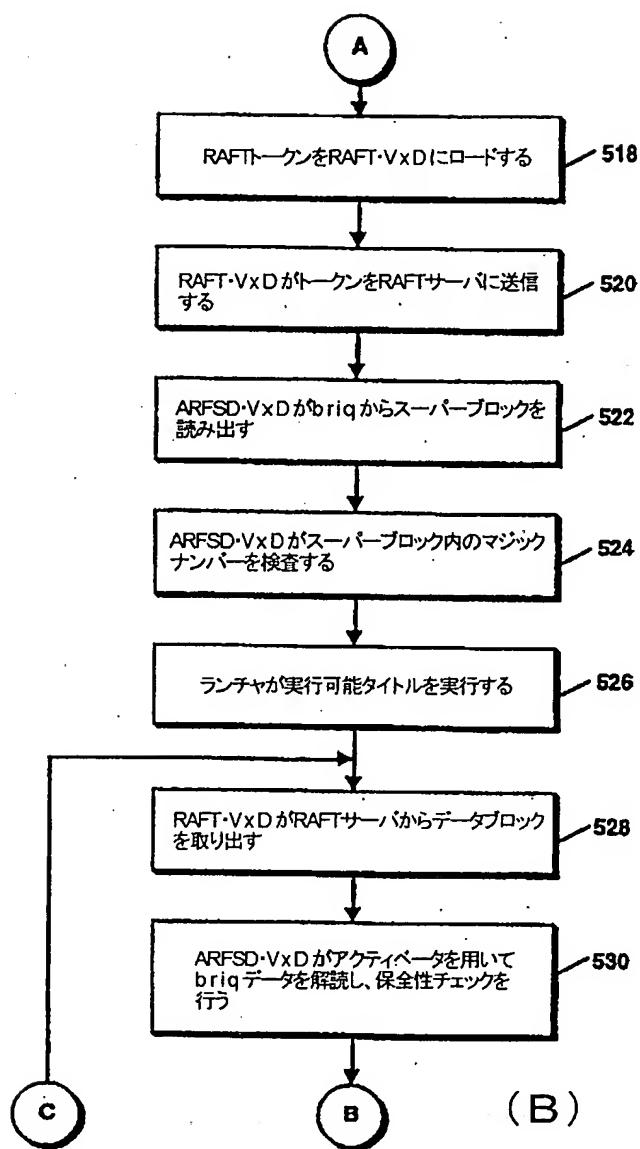
【図4B】



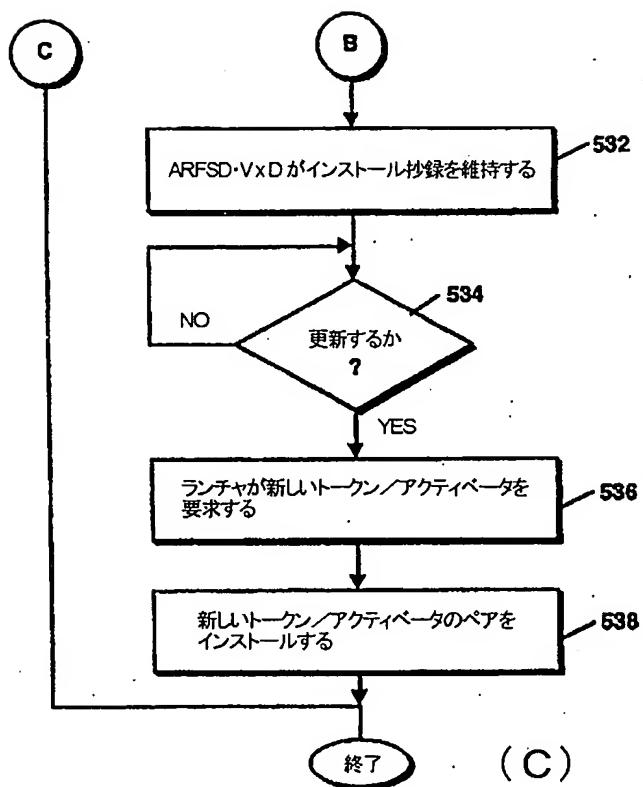
【図5A】



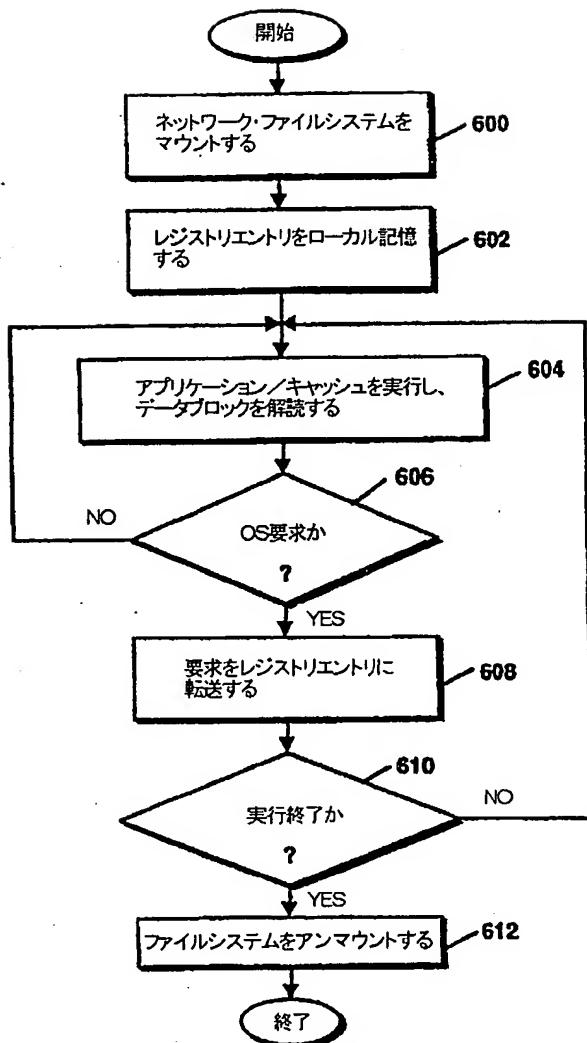
【図 5 B】



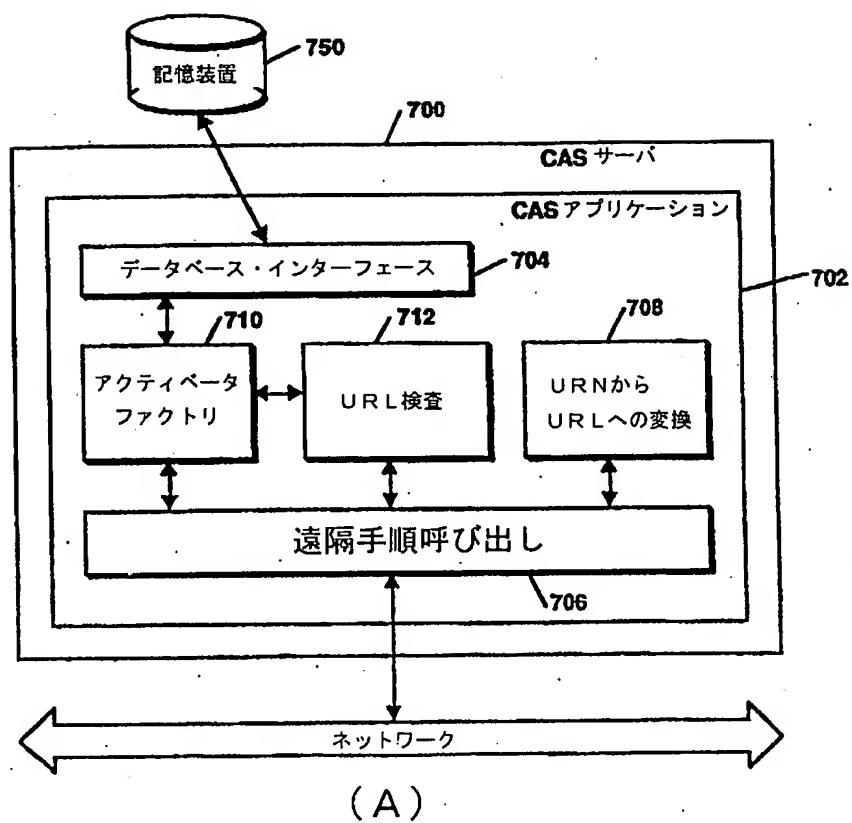
【図 5 C】



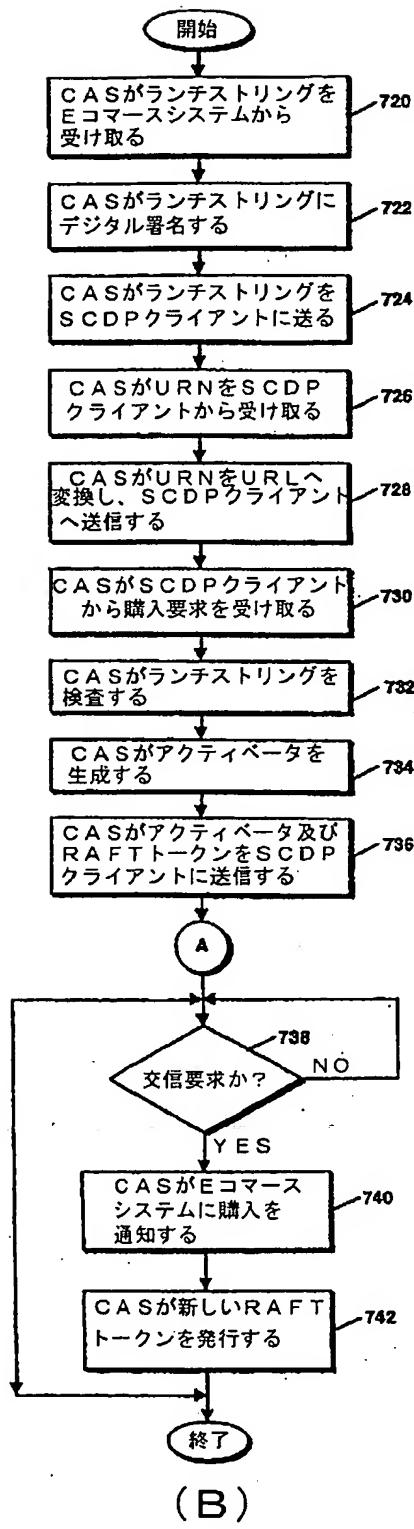
【図6】



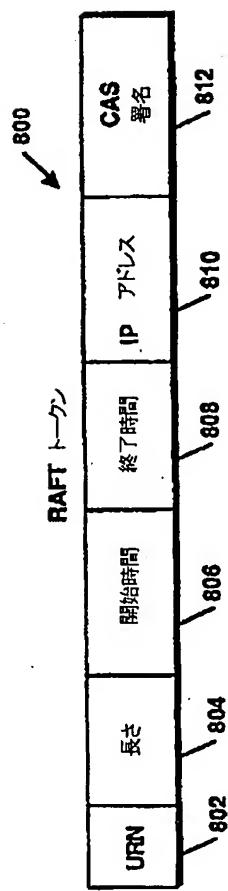
【図 7 A】



【図 7 B】



【図 8】

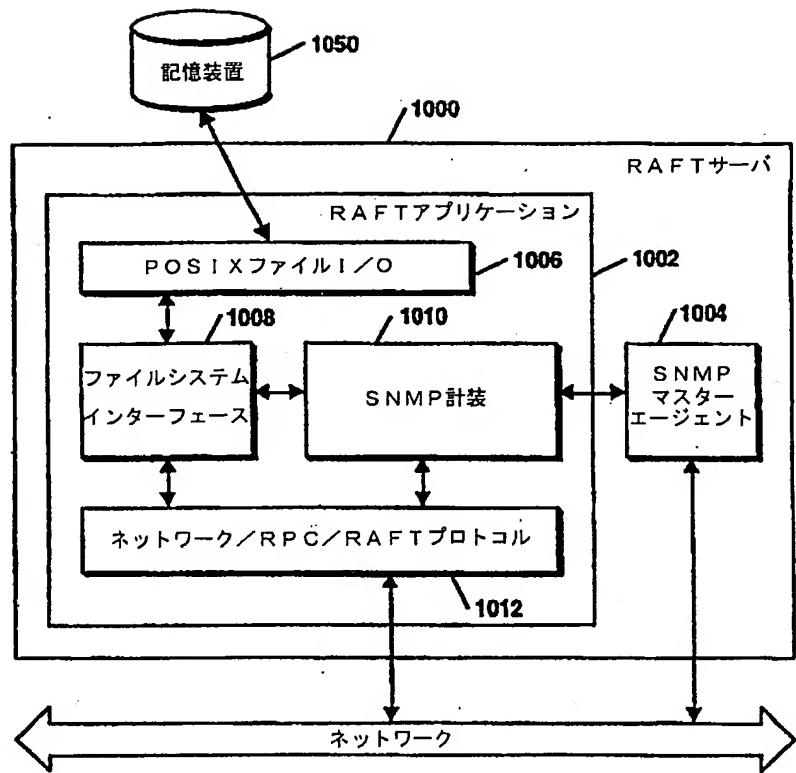


【図9】

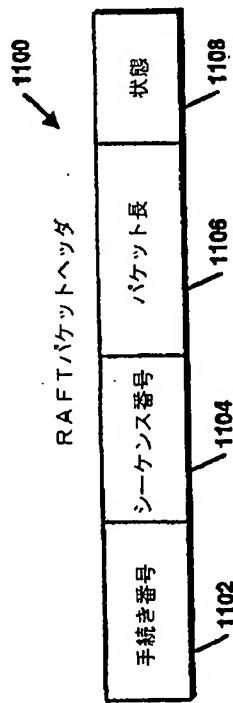
データストリップ

URN	店舗ID	商品タイプ	加入メイン	金額	CAS 署名
902	904	906	908	910	912

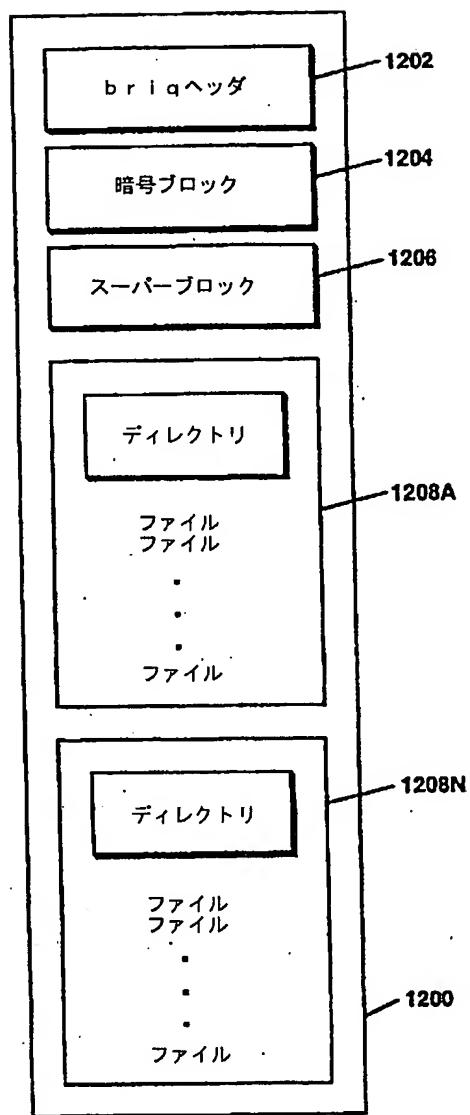
【図10】



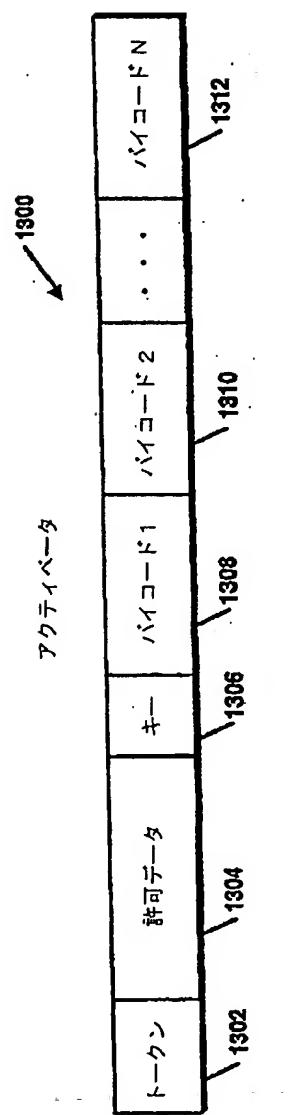
【図11】



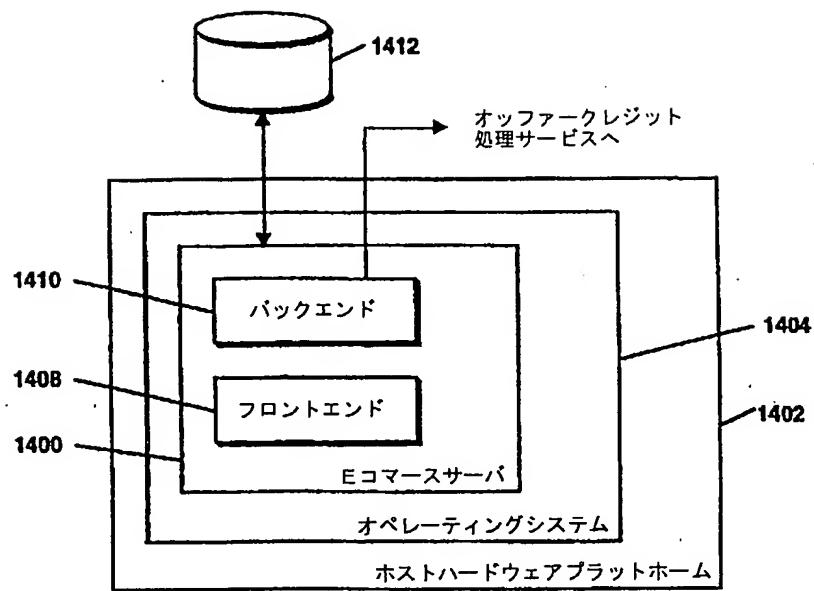
【図12】



【図13】



【図14】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inte...inal Application No
PCT/US 99/27113

A. CLASSIFICATION OF SUBJECT MATTER		
IPC 7 H04L29/06 G06F9/45		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) IPC 7 H04L G06F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indicator, where appropriate, of the relevant passages	Relevant to claim No.
P, X	<p>WO 99 45491 A (NUVOMEDIA INC) 10 September 1999 (1999-09-10) abstract page 1, line 7 - line 11 page 2, line 31 - page 3, line 4 page 4, line 9 - line 27 page 5, line 28 - line 32 page 7, line 2 - line 6 page 7, line 25 - line 31 page 15; claim 1</p> <p style="text-align: center;">-/-</p>	1,5
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C.		<input checked="" type="checkbox"/> Patent family members are listed in annex.
<p>* Special categories of cited documents :</p> <p>'A' document defining the general state of the art which is not considered to be of particular relevance</p> <p>'E' earlier document but published on or after the International filing date</p> <p>'U' document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>'O' document referring to an oral disclosure, use, exhibition or other means</p> <p>'P' document published prior to the International filing date but later than the priority date claimed</p> <p>'T' later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>'Y' document of particular relevance; the claimed invention can not be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>'M' document member of the same patent family</p>		
Date of the actual completion of the International search	Date of mailing of the International search report	
30 May 2000	07/06/2000	
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentzaan 2 NL-1280 HV Rijswijk Tel: (+31-70) 340-2040, Tx: 91 651 opo nl Fax: (+31-70) 340-3018	Authorized officer Adkhis, F	

Form PCT/ISA/2.10 (second sheet) (July 1992)

page 1 of 2

INTERNATIONAL SEARCH REPORT

Int'l Application No
PCT/US 99/27113

C./Continuation DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>RUBIN A D: "Secure distribution of electronic documents in a hostile environment" COMPUTER COMMUNICATIONS, NL, ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, vol. 18, no. 6, 1 June 1995 (1995-06-01), pages 429-434, XP004032475 ISSN: 0140-3664 abstract page 430, right-hand column, line 9 – line 43 page 431, left-hand column, line 35 – line 57</p>	1-21

Form PCT/ADA/210 (continuation of second sheet) (July 1992)

page 2 of 2

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int'l. Appl. No.
PCT/US 99/27113

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9945491 A	10-09-1999	WO 0021239 A	13-04-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

 フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	マークコード(参考)
G 0 6 F 17/30	1 2 0	G 0 6 F 9/06	6 6 0 C
			6 6 0 G

- (31) 優先権主張番号 0 9 / 3 1 1, 9 2 3
 (32) 優先日 平成11年5月12日(1999. 5. 12)
 (33) 優先権主張国 米国(US)
 (31) 優先権主張番号 0 9 / 3 1 0, 2 2 9
 (32) 優先日 平成11年5月12日(1999. 5. 12)
 (33) 優先権主張国 米国(US)
 (31) 優先権主張番号 0 9 / 4 3 9, 9 0 6
 (32) 優先日 平成11年11月12日(1999. 11. 12)
 (33) 優先権主張国 米国(US)
 (81) 指定国 E P (A T, B E, C H, C Y,
 D E, D K, E S, F I, F R, G B, G R, I E, I
 T, L U, M C, N L, P T, S E), A U, C A, C
 N, J P, K R, S G, Z A
 (72) 発明者 エイチン・マーク ダブリュー
 アメリカ合衆国 マサチューセッツ州
 02144 サマービル シャープ331 ハイラ
 ンド アベニュー 411エー
 (72) 発明者 ロストチェック デービッド ジェイ
 アメリカ合衆国 マサチューセッツ州
 02474 アーリントン ブルックデール
 ロード 9
 F ターム(参考) 5B017 AA03 BA07 BB10 CA15
 5B075 KK43 KK54 NK04 PQ05
 5B076 FB01
 5B082 EA12 GA11 HA05